Mathematics and Engineering Physics

CM elliptic curves and the Coates–Wiles Theorem

Author:
Martí Roset

Advisor:
Francesc Fité

Advisor (UPC):
Víctor Rotger

February 8, 2019

Abstract

We present one of the only known cases of the Birch and Swinnerton-Dyer Conjecture, the so called Coates–Wiles Theorem. Let K be an imaginary quadratic field with ring of integers $\mathcal{O}$ and let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by $\mathcal{O}$. The Coates–Wiles Theorem states that if the L-series attached to $E/\mathbb{Q}$ does not vanish at 1 then the set of rational points of E is finite.

We explain a proof given by Karl Rubin, which uses the theory of Euler systems. We begin the exposition reviewing the basic theory of elliptic curves over local fields and elliptic curves with complex multiplication. After that, we study the Euler system of elliptic units and its connection with the L-series attached to E.

Keywords

BSD Conjecture, Coates–Wiles Theorem, L-series, elliptic curves with CM, Euler systems, elliptic units.

Contents

Acknowledgments

I would like to start expressing my very great appreciation to Francesc Fité. He has been extremely generous with his time as well as patient when giving me advice about the project. In addition, he transmitted his passion about number theory and research in every talk we had which has motivated me a lot in my first steps in this subject. I would also like to thank Christopher Skinner for giving me the opportunity of visiting Princeton University for 6 months and for being available whenever I needed. My thanks are also extended to Víctor Rotger for purposing me to work on this project.

I would like to express my gratitude to CFIS and Fundació CELLEX for organizing and partially founding this mobility program. Also to the staff from Princeton University and CFIS for making things easier. I am also very thankful to the people from the Department of Mathematics of Princeton University for being always very nice and ready to help me: Javier Gómez Serrano, Francesc Castellà, the graduate students and the visiting students.

Finally, I wish to thank my friends and my family, for all the good times I have spent working with them and for their support and encouragement during this period.

Introduction

An elliptic curve E defined over a field F is a algebraic projective nonsingular curve of genus one with a distinguished point O. The Riemann–Roch Theorem shows that the set of affine F-rational points of E can be identified with the locus of solutions in $\mathbb{A}^2(F)$ of a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

where the coefficients $a_i \in F$. Then, O is the point at infinity. We will denote by $E(F)$ the set of points $P = (x, y)$ with $x, y \in F$ that satisfy (1) together with the point O.

Remarkably, $E(F)$ can be endowed with a natural group structure. It is given by the Chord-Tangent Method. Given two points $P, Q \in E(F)$, consider the point R of intersection of the line passing through P and Q with $E(F)$. Then, define $P + Q$ to be the intersection of the line through R and O with $E(F)$.

The endomorphisms of E are the morphisms $\phi : E \to E$ of algebraic curves that respect the group structure of E. The set $\mathrm{End}(E)$ of endomorphisms of E is a ring where the operations are addition and composition. Some examples of endomorphisms are the maps multiplication-by-m for some integer m, which are naturally defined by adding a point m times using the Chord-Tangent Method. For some curves these are all the possible endomorphisms. For others, $\mathrm{End}(E)$ can have more elements, in that case we say that E has complex multiplication: the ring $\mathrm{End}(E)$ can be either an order in an imaginary quadratic field or a quaternion algebra, and this last option is not possible if F has characteristic 0.

From now on assume that F is a number field with ring of integers $\mathcal{O}_F$. It is natural to ask about the size of $E(F)$ and it results that we can use the group structure of $E(F)$ to say something about it. A very important example of what we just said is the Mordell–Weil Theorem which states that $E(F)$ is a finitely generated group, i.e. $E(F) \cong \mathbb{Z}^r \oplus T$ where $r \geq 0$ is an integer and T is a finite group. We call $r = r_E$ the rank of E, a mysterious invariant that has been object of extensive study.

Based on computer calculations, a conjectural answer to find r_E was given by Birch and Swinnerton-Dyer in 1965, the so called BSD conjecture. It connects the algebraic nature of r_E with an analytic object attached to E, the L-series. Suppose that every $a_i \in \mathcal{O}_F$. The L-series attached to E is defined by an infinite product over the prime ideals of $\mathcal{O}_F$

$$L(E_{/F}, s) = \prod_{\mathfrak{p}} \frac{1}{L_{\mathfrak{p}}(E_{/F}, \mathrm{N}\mathfrak{p}^{-s})},$$

where $L_{\mathfrak{p}}(E_{/F}, T)$ is a polynomial of degree ≤ 2 and it is called the local factor at $\mathfrak{p}$. To define it, consider (1) reduced modulo $\mathfrak{p}$ (the reader should notice that the curve

we obtain depends on the choice of the Weierstrass equation, we will explain how to define this reduction in the first chapter). It was proven by Hasse that whenever the reduced equation is an elliptic curve over the field $\mathbb{F}_{\mathrm{N}\mathfrak{p}}$, which we will denote by $\tilde{E}(\mathbb{F}_{\mathrm{N}\mathfrak{p}})$, we have

$$\#\tilde{E}(\mathbb{F}_{\mathrm{N}\mathfrak{p}}) = \mathrm{N}\mathfrak{p} - a_{\mathfrak{p}} + 1,$$

where $-2\sqrt{\mathrm{N}\mathfrak{p}} \leq a_{\mathfrak{p}} \leq 2\sqrt{\mathrm{N}\mathfrak{p}}$. In that case, we define $L_p(E_{/F}, T) = (1 - a_{\mathfrak{p}}T + \mathrm{N}\mathfrak{p}T^2)$. When the reduced curve is not an elliptic curve the definition for $L_{\mathfrak{p}}(E_{/F}, T)$ depends on the structure of the group of nonsingular points of $\tilde{E}(\mathbb{F}_p)$.

Using the estimate of $a_{\mathfrak{p}}$ it is not hard to see that the Euler product converges on the right half plane $\{s \in \mathbb{C} : \mathrm{Re}(s) > 3/2\}$. Birch and Swinnerton-Dyer conjectured the following.

Conjecture (BSD Conjecture)**.** *The series $L(E_{/F}, s)$ admits an analytic continuation to the entire complex plane, Moreover*

$$r_E = \mathrm{ord}_{s=1} L(E_{/F}, s).$$

At this point is worth mentioning the local global principle. The definition of the L-series attached to E has information of the curve E defined over the residue fields $\mathbb{F}_{\mathrm{N}\mathfrak{p}}$, which we can call local information, and the BSD Conjecture states that it is possible to deduce results of E over the global field F from it.

For the case where $F = \mathbb{Q}$ the work of Wiles et al. on the Shimura–Tanyiama–Weil Conjecture implies that $L(E_{/\mathbb{Q}}, s)$ has analytic continuation. The analytic continuation for the particular case where E has complex multiplication is known since the work of Deuring, who gave an expression of $L(E_{/F}, s)$ in terms of the so called Hecke L-series (as we will see in Chapter 7) and Hecke who proved the analytic continuation of Hecke L-series. In this project we prove one particular case of the BSD Conjecture.

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}$ and class number 1.

Theorem (Coates–Wiles)**.** *Suppose E is defined over $\mathbb{Q}$ and it has complex multiplication by $\mathcal{O}$. If $L(E_{/\mathbb{Q}}, 1) \neq 0$ then $E(\mathbb{Q})$ is finite.*

We will actually prove the following result. Suppose E is defined over K and it has complex multiplication by $\mathcal{O}$. If $L(E_{/K}, 1) \neq 0$ then $E(K)$ is finite. In Chapter 7 we will see that this result implies the desired theorem (in fact the two statements are equivalent).

We will expose a proof of this theorem given by Rubin in [Rub99]. As we said, the analytic continuation of the L-series for our particular case was already known at this time so we will focus on proving that $E(K)$ is a finite group. Our exposition is organized in the following manner.

Chapters 1 and 2 are introductory. In the first one we study elliptic curves over local fields with a discrete valuation while in the second one we study elliptic curves over $\mathbb{C}$. In the second part of Chapter 2 we discuss the theory of elliptic curves with complex multiplication. We do it in detail since this theory is essential for the rest of the exposition.

Chapter 3 consists on giving an expression of the Selmer group of certain endomorphisms which will allow us to determine when it they are trivial. This is the characterization that we will use in order to prove that $E(K)$ is finite.

Chapters 4, 5 and 6 cover the theory of the Euler system of elliptic units. We introduce this system and explain how it is used to bound certain ideal class groups.

Chapter 7 explains the connection between elliptic units and the L-series of E.

Finally, Chapter 8 combines the previous work to prove the theorem. It shows that if $L(E_{/K}, 1) \neq 0$, we can produce a concrete system of elliptic units. Applying the theory of Euler systems to it we will be able to give a sharp bound of the ideal class group studied in Chapter 6. This is precisely one of the conditions to show that certain Selmer group is trivial and with some additional work we will be able to conclude the proof.

Recommended background

We will assume the knowledge of an introductory course on algebraic number theory, for example [Sam70]. The basic results about local fields are also assumed as well as the main results of local and global class field theory. A very concise document with most of the statements that we will use is [Poo], for a detailed exposition of the topic see [Mil13]. We also use freely the basic results of an introductory course on elliptic curves, for example [Sil09]. However, in the first two chapters we review some parts of this book that will be very relevant for us.

Chapter 1

Elliptic curves over local fields and the formal group

When studying a concrete equation over a number field it is natural to consider the reduced equation modulo some prime. The existence of solutions and its structre on the residue field can tell us information about the original equation. More precisely, we can obtain information about the equation over the completion of the number field with respect to this prime and sometimes this can be translated to information about the original equation over the number field.

In this chapter we present the basic results of elliptic curves over local fields with discrete valuation. To do it we introduce a basic tool to study them: the formal group. After that, we define the corresponding formal group of an elliptic curve which allow us to apply the results of formal groups to elliptic curves. We will be able to extract information about the structure of the points of the curve and about the field extensions generated by some torsion points.

We follow [Sil09] Chapters IV and VII for the first sections and [Rub99] for the last one.

Suppose that K is a local field with respect to a discrete valuation, let $\mathcal{O}$ be its ring of integers and $\pi \in \mathcal{O}$ a uniformizer such that $(\pi) = \mathfrak{p}$ is the maximal ideal of $\mathcal{O}$. Denote by k the residue field of K and let p be its characteristic.

1.1 Formal groups

Let R be a ring.

Definition 1.1.1. A formal group $\mathcal{F}$ over R is a power series $F \in R[[X, Y]]$ of the form $F(X, Y) = X + Y + O(X^2, Y^2, XY)$ satisfying:

1. Associativity: $F(X, F(Y, Z)) = F(F(X, Y), Z)$.

2. Commutativity: $F(X, Y) = F(Y, X)$.

3. Inverses: There exists a unique power series $i(T) \in R[[T]]$ such that $F(T, i(T)) = F(i(T), T) = 0$.

4. Neutral element: $F(X, 0) = X$ and $F(0, Y) = Y$.

Example 1.1.2. The easiest examples of formal groups over R are the additive formal group $\mathbb{G}_a$, with formal group law $F(X, Y) = X + Y$, and the multiplicative formal group $\mathbb{G}_m$, with formal group law $F(X, Y) = X + Y + XY$.

We can define morphisms between formal groups.

Definition 1.1.3. Let $\mathcal{F}, \mathcal{G}$ be formal groups over R with group laws $F(X, Y), G(X, Y) \in R[[X, Y]]$ respectively.

1. A morphism from $\mathcal{F}$ to $\mathcal{G}$ is a power series $f(T) \in TR[[T]]$ satisfying

$$f(F(X, Y)) = G(f(X), f(Y)).$$

2. An isomorphism of the formal groups $\mathcal{F}$ and $\mathcal{G}$ is a morphism $f(T)$ from $\mathcal{F}$ to $\mathcal{G}$ such that there exists $g(T) \in TR[[T]]$ such that

$$f(g(T)) = g(f(T)) = T.$$

Example 1.1.4. One important example is the endomorphism multiplication-by-m, where $m \in \mathbb{Z}$. Let $[0](T) = 0$. Then, define $[m](T) \in TR[[T]]$ as

$$[m + 1](T) = F([m]T, T), \quad [m - 1](T) = F([m](T), i(T)).$$

By induction, it is not hard to see that this is an endomorphism of the formal group $\mathcal{F}$ with formal group law $F(X, Y)$ and that $[m](T) = mT + O(T^2)$.

As in the ring of power series with the product, it is easy to characterize when a morphism has inverse with respect to composition.

Proposition 1.1.5. *Let $f(T) = aT + O(T^2) \in R[[T]]$. Then, $a \in R^\times$ if and only if there exists a unique power series $g(T) \in TR[[T]]$ such that*

$$f(g(T)) = g(f(T)) = T.$$

Proof. One implication is clear, for the other one suppose that $a \in R^\times$. Define a sequence of polynomials $g_n(T) \in R[T]$ of degree n such that $g_{n+1}(T) \equiv g_n(T) \mod T^n$ and $f(g_n(T)) \equiv T \mod T^{n+1}$ for every $n \geq 1$. We do it inductively by taking $g_1(T) = a^{-1}T$ and, if we write $g_{n+1}(T) = g_n(T) + bT^{n+1}$ we can determine b using the condition $f(g_{n+1}(T)) \equiv T \mod T^{n+2}$. Indeed

$$f(g_n(T) + bT^{n+1}) = f(g_n(T)) + abT^{n+1} + O(T^{n+2}) \equiv f(g_n(T)) + abT^{n+1} \mod T^{n+2}.$$

By the inductive hypothesis, $f(g_n(T)) \equiv T + b'T^{n+1}$ so we just need to choose $b = -a^{-1}b'$. The desired $g(T)$ is the limit of the polynomials $(g_n(T))$.

We are left to see that $g(f(T)) = T$. Since $g'(0) \in R^\times$ (prime stands for derivative), using what we just proved, there exists $h(T)$ such that $g(h(T)) = T$. Then

$$g(f(T)) = g(f(g(h(T))) = g(f \circ g(h(T))) = g(h(T)) = T.$$

For the uniqueness, if $h(T)$ also satisfies this conditions $h(T) = h(f(g(T))) = g(T)$. □

Corollary 1.1.6. *Let $\mathcal{F}/R$ and $\mathcal{G}/R$ be formal groups, $F(X,Y), G(X,Y) \in R[[X,Y]]$ their group laws respectively. Suppose that $f(T) = aT + O(T^2)$ is a morphism from $\mathcal{F}$ to $\mathcal{G}$ and $a \in R^\times$. Then $f(T)$ is an isomorphism.*

In particular, if $m \in \mathbb{Z}$ is a unit in R the multiplication-by-m map $[m]$ is an automorphism.

Proof. By the previous proposition there exists $g(T) \in TR[T]$ such that $f(g(T)) = g(f(T)) = T$. □

From now on suppose that $R = \mathcal{O}$, the ring of integers of the local field K and let $\mathcal{F}$ be a formal group over $\mathcal{O}$ with formal group law $F(X,Y) \in \mathcal{O}[[Z]]$. It will become clear why we need to assume this.

As we explained, $\mathcal{F}$ is a group law $F(X,Y) \in \mathcal{O}[[X,Y]]$ without elements. Note that if $x, y \in \mathfrak{p}$ we can evaluate $F(x,y)$, since the series converges with respect to the norm induced by the valuation (note that it converges to an element of $\mathfrak{p}$). In a similar way $i(x) \in \mathfrak{p}$ because $i(T) = -T + O(T^2)$ (this is a consequence of $F(T, i(T))$) and also $F(x, i(x)) = 0$. We can therefore construct a group where addition is specified by $F(X,Y)$.

Definition 1.1.7. The group associated to $\mathcal{F}/\mathcal{O}$, denoted by $\mathcal{F}(\mathfrak{p})$ is the set $\mathfrak{p}$ endowed with the group operations

$$x \oplus_{\mathcal{F}} y = F(x,y), \quad \ominus_{\mathcal{F}} x = i(x)$$

for all $x, y \in \mathfrak{p}$.

Proposition 1.1.8. *Let $\mathcal{F}, \mathcal{G}$ be a formal groups over $\mathcal{O}$ with formal group laws $F(X,Y), G(X,Y) \in \mathcal{O}[[X,Y]]$. Then, any morphism $f(T) \in T\mathcal{O}[[T]]$ from $\mathcal{F}$ to $\mathcal{G}$ induces naturally a morphism of the associated groups $f : \mathcal{F}(\mathfrak{p}) \to \mathcal{G}(\mathfrak{p})$.*

Proof. The morphism is just evaluation of the power series. It is clear that it converges and that it is a morphism. □

Corollary 1.1.9. *Every element of finite order in $\mathcal{F}(\mathfrak{p})$ has order a power of p.*

Proof. It is enough to prove that there is no nontrivial element of order coprime to p. For that, let $m \in \mathbb{Z}$ such that $(m,p) = 1$ and consider the morphism of the formal groups multiplication-by-m. Since $m \in \mathcal{O}^\times$, Corollary 1.1.6 shows that it is an isomorphism of formal groups so by the previous proposition multiplication-by-m is an isomorphism of the associated groups. Hence, its kernel is trivial. □

It is possible to say even more about the torsion subgroup of $\mathcal{F}(\mathfrak{p})$. In fact, in some cases it is possible to determine the structure of the group $\mathcal{F}(\mathfrak{p})$. In order to do it we will define a logarithm that will be a morphism of formal groups between $\mathcal{F}$ and the additive group $\mathbb{G}_a$. Then, we will study in which cases this morphism becomes an isomorphism of the associated groups, $\mathcal{F}(\mathfrak{p})$ and $\mathbb{G}_a(\mathfrak{p}) \cong \mathfrak{p}\mathcal{O}$ obtaining the desired structure of $\mathcal{F}(\mathfrak{p})$.

Remark 1.1.10. What we just described is a generalization of the process that is done to study the structure of the nth higher unit groups $U^{(n)} = 1 + \mathfrak{p}^n \subset \mathcal{O}^\times$ of the local field K using the logarithm map. In fact, taking $\mathcal{F} = \mathbb{G}_m$, the associated group $\mathbb{G}_m(\mathfrak{p}) \cong U^{(1)}$ and one recovers the well known results for the structure of $U^{(n)}$ for local fields.

The next proposition is an example of what we just said in the remark: it is a well known result for the nth higher unit groups of a local field $U^{(n)}$ and now we see that it is, in fact, a general result of formal groups.

Proposition 1.1.11. *Let $\mathcal{F}$ be the associated group to F. For $n \geq 1$ the natural map*

$$\mathcal{F}(\mathfrak{p}^n)/\mathcal{F}(\mathfrak{p}^{n+1}) \to \mathfrak{p}^n/\mathfrak{p}^{n+1}$$

is an isomorphism.

Proof. It is clear that the map is well defined. To show that it is a morphism one just have to note that $F(X,Y) = X + Y + O(X^2, Y^2, XY)$. Therefore, if $x, y \in \mathfrak{p}^n$ with $n \geq 1$ it is plain that $F(x,y) \equiv x + y \mod \mathfrak{p}^{n+1}$. □

We proced to define the invariant differential of a formal group $\mathcal{F}$. This will allow us to define the logarithm.

Definition 1.1.12. An invariant differential ω of the formal group $\mathcal{F}/\mathcal{O}$ with formal group law $F(X,Y)$ is a differential form

$$\omega(T) = P(T)dT \in \mathcal{O}[[T]]dT$$

such that it is invariant under addition, i.e.

$$\omega(F(T,S)) = \omega(T),$$

where T and S are variables.

Proposition 1.1.13. *For a given $\mathcal{F}/\mathcal{O}$ formal group with formal group law F there exists a unique normalized invariant diferential (i.e. $P(0) = 1$) and it is of the form*

$$\omega(T) = F_X(0,T)^{-1}dT,$$

where $F_X(X,Y)$ stands for the derivative of $F(X,Y)$ with respect to the first component. Moreover, all invariant differentials are of the form $c\omega(T)$ with $c \in \mathcal{O}$.

Proof. If $\omega(T) = P(T)dT$ is an invariant differential

$$P(F(T,S)d(F(T,S)) = P(T)dT$$

which implies

$$P(F(T,S))F_X(T,S) = P(T).$$

Taking $T = 0$ we get

$$P(S)F_X(0,S) = P(0)$$

and since $F(X,Y) = X + Y + O(X^2, Y^2, XY)$, we have $F_X(0,S) = 1 + O(S)$ and hence $F_X(0,S)$ is invertible. Therefore

$$P(S) = P(0)F_X(0,S)^{-1}.$$

so any invariant differential has to be of the form

$$\omega(T) = cF_X(0,T)^{-1}dT.$$

To conclude the proof we are left to see that $\omega(T) = F_X(0,T)^{-1}dT$ is an invariant differential. This is obtained differentiating the associative law with respect to U

$$F(U,F(T,S)) = F(F(U,T),S).$$

□

The following is an easy consequence of the uniquenes of the invariant differential.

Corollary 1.1.14. *Let $\mathcal{F}$ and $\mathcal{G}$ be formal groups over $\mathcal{O}$ with formal group laws $F(X,Y), G(X,Y) \in \mathcal{O}[[T]]$ respectively. Let $f \in T\mathcal{O}[[T]]$ be a morphism from $\mathcal{F}$ to $\mathcal{G}$. Then, if $\omega_{\mathcal{F}}$ and $\omega_{\mathcal{G}}$ are normalized invariant differentials of $\mathcal{F}$ and $\mathcal{G}$ respectively*

$$\omega_{\mathcal{G}} \circ f = f'(0)\omega_{\mathcal{F}}.$$

Proof. We first see that $\omega_{\mathcal{G}} \circ f$ is an invariant differential of $\mathcal{F}$. If T, S are variables

$$\omega_{\mathcal{G}}(f(F(T,S))) = \omega_{\mathcal{G}}(G(f(T), f(S)) = \omega_{\mathcal{G}}(f(T)).$$

Hence $\omega_{\mathcal{G}} \circ f = c\omega_{\mathcal{F}}$ for some $c \in \mathcal{O}$. To determine c, use the expression of the normalized invariant differentials

$$G_X(0, f(T))^{-1} f'(T) dT = cF_X(0,T)^{-1} dT$$

and since $F_X(0,T) = 1 + O(T), G_X(0,T) = 1 + O(T)$ (see the expression of the formal group law in Definition 1.1.1), evaluation at $T = 0$ leads to $c = f'(0)$. □

The fact that $\omega(T)$ is invariant under addition using the formal group law F is the key for defining a logarithm. From now on we also assume that $\mathrm{char}(K) = 0$.

Proposition 1.1.15. *Denote by ω the normalized invariant differential of $\mathcal{F}/\mathcal{O}$. Define the formal logarithm of $\mathcal{F}/\mathcal{O}$ as*

$$\log_{\mathcal{F}}(T) = \int \omega(T) \in K[[T]]$$

Remark 1.1.16. In the process of integrating $\omega(T)$ some denominators will appear. Therefore the power series $\log_{\mathcal{F}}(T)$ will be a morphism of formal groups over the ring K.

Proposition 1.1.17. *The power series $\log_{\mathcal{F}}(T) \in K[[T]]$ is an isomorphism between the formal groups $\mathcal{F}$ and $\mathbb{G}_a$ seen as formal groups over K. We will call $\exp_{\mathcal{F}}(T)$ to its inverse.*

Proof. Since the normalized invariant differential $\omega(T) = P(T)dT = F_X(0,T)^{-1}dT = (1 + O(T))dT$, the formal logarithm is of the form $\log_{\mathcal{F}}(T) = T + O(T^2) \in TK[[T]]$. To see that it is a morphism we are left with proving

$$\log_F(F(T,S)) = \log_{\mathcal{F}}(T) + \log_{\mathcal{F}}(S).$$

To do it, we use that ω is an invariant differntial

$$P(F(T,S))d(F(T,S)) = P(T)dT,$$

integrating this with respect to T

$$\log_{\mathcal{F}}(F(T,S)) = \log_{\mathcal{F}}(T) + C(S).$$

To determine $C(S)$ just take $T = 0$ and use that $\log_{\mathcal{F}}(0) = 0$. Hence $C(S) = \log_{\mathcal{F}}(S)$. Finally, we can apply Corollary 1.1.6 to see that $\log_{\mathcal{F}}(T)$ has an inverse with coefficients defined over K. □

The next step is to see when this isomorphism can induce an isomorphism of the groups $\mathcal{F}(\mathfrak{p})$ and $\mathbb{G}_a(\mathfrak{p})$. This can be done by studying the expresions of the series $\log_F(T)$ and $\exp_F(T)$ to see for which $z \in \mathfrak{p}$ they converge. We just state the final result without a complete proof.

Lemma 1.1.18. *The series* $\log_{\mathcal{F}}$ *and* $\exp_{\mathcal{F}}$ *are of the form*

$$\log_{\mathcal{F}}(T) = \sum_{n=1}^{\infty} \frac{a_n}{n} T^n, \quad \exp_{\mathcal{F}}(T) = \sum_{n=1}^{\infty} \frac{b_n}{n!} T^n,$$

with $a_n, b_n \in \mathcal{O}$ *for all* n.

Therefore, if $z \in \mathfrak{p}$, $\log_{\mathcal{F}}(z)$ *converges to an element of* $\mathfrak{p}$. *If* $v(z) > v(p)/(p-1)$ *then* $\exp_{\mathcal{F}}(z)$ *also converges to an element of order* $v(z)$.

Proof. Since the power series of $\omega(T)$ has coefficients in $\mathcal{O}[[T]]$ it is clear that its integral, $\log_{\mathcal{F}}(T)$, has the form stated in this proposition. From here it is easy to see that if $z \in \mathfrak{p}$, $\log_{\mathcal{F}}(z)$ will converge.

For $\exp_{\mathcal{F}}(T)$ one has to first prove the expression of the power series and then study its convergence. This can be found in [Sil09] Chapter 4, Proposition 5.5 and Lemma 6.3. □

Theorem 1.1.19. *If* $r > v(p)/(p-1)$ *the formal logarithm induces an isomorphism*

$$\log_{\mathcal{F}} : \mathcal{F}(\mathfrak{p}^r) \to \mathbb{G}_a(\mathfrak{p}^r)$$

whose inverse is the morphism induced by the power series $\exp_{\mathcal{F}}(T)$.

Proof. In Proposition 1.1.17 we proved that $\log_{\mathcal{F}}(T)$ is an isomorphism of formal groups, so if we restrict to a set where both $\log_{\mathcal{F}}(T)$ and $\exp_{\mathcal{F}}(T)$ converge we naturally obtain an isomorphism of the associated subgroups. Thus, the result follows from Lemma 1.1.18. □

1.2 The formal group associated to an elliptic curve

We now introduce the formal group of an elliptic curve. This could be defined for curves over an arbitrary field. However, as we saw in the previous section, if we want to consider the group attached to the formal group we will be interested in formal groups over a local ring. Therefore we assume that E is an elliptic curve defined over K and we fix a Weierstrass equation for E

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Making the substitution $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ we obtain an isomorphic curve with coefficients $u^i a_i$. Therefore, it is possible to choose $u \in K$ such that all the coefficients of the Weierstrass equation are in $\mathcal{O}$. Assume therefore that $a_i \in \mathcal{O}$ for every i.

Note that a point in the projective curve with coordinates $[X, Y, Z]$ and $Y \neq 0$ satisfies, $[X, Y, Z] = [X/Y, 1, Z/Y]$. This motivates the following change of variables

$$z = -\frac{x}{y}, \quad w = -\frac{1}{y} \tag{1.1}$$

where the point at infinity corresponds to $(0, 0)$. Now the Weierstrass equation has the form

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 = f(z, w). \tag{1.2}$$

We can take the equation $w = f(z, w)$ and substitute it in the expression of w as an argument of f obtaining the equation $w = f(z, f(z, w))$. Repeating this process leads to a power series with coefficients in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6] \subset \mathcal{O}$ that expresses w in terms of z. Using Hensel's Lemma on the ring $\mathbb{Z}[a_1, \ldots, a_6][[Z]]$, which is complete with respet to the maximal ideal (Z), one proves that this power series is well defined and that it is unique.

Proposition 1.2.1. *There exists a unique power series $w(Z) \in \mathcal{O}[[Z]]$ such that $w(Z) = f(Z, w(Z))$. In fact, $w(Z)$ is of the form $w(Z) = Z^3(1 + A_1Z + A_2Z + \ldots) \in Z^3\mathcal{O}[[Z]]$ with $A_i \in \mathcal{O}$.*

Proof. See [Sil09] Chapter IV Proposition 1.1. □

Computing the expression of $w(Z)$ and using the formulas of (1.1) one obtains the following expressions for $x(Z), y(Z)$:

$$x(Z) = Z/w(Z) = 1/Z^2 - a_1/Z - a_2 - a_3Z - (a_4 + a_1a_3)Z^2 + \cdots \in Z^{-2}\mathcal{O}[[Z]], \tag{1.3}$$

$$y(Z) = -1/w(Z) = -1/Z^3 + a_1/Z^2 + a_2/Z + a_3 + (a_4 + a_1a_3)Z + \cdots \in Z^{-3}\mathcal{O}[[Z]]. \tag{1.4}$$

Remark 1.2.2. Another way to justify thiese expressions for $x(Z), y(Z)$ is to note that $z = -x/y$ is a uniformizer of the local ring of functions $K[E]_O$, so we can write the coordinate funtions x, y (in fact every rational function) in terms of z in the completion of this ring.

By construction it is clear that $x(Z), y(Z)$ will satisfy the Weierstrass equation for E as power series. This allows us to define formally the addition of the "points" $(x(Z_1), y(Z_1))$ and $(x(Z_2), y(Z_2))$ using the addition formula for points of E (following the geometric law) and it is possible to compute the result in terms of Z_1, Z_2. Similarly one can compute compute the inverse of $(x(Z), y(Z))$ in terms of Z.

Proposition 1.2.3. *For the curve E with Weierstrass coordinate functions x, y and power series $x(Z), y(Z)$ we have:*

1. *There exists a unique power series $F(Z_1, Z_2) = Z_1 + Z_2 + O(Z_1^2, Z_2^2, Z_1 Z_2) \in \mathcal{O}[[Z_1, Z_2]]$ such that*

$$(x(Z_1), y(Z_1)) + (x(Z_2), y(Z_2)) = (x(Z_3), y(Z_3))$$

   where $Z_3 = F(Z_1, Z_2)$.

2. *There exists a unique power series $i(Z) = -Z + O(Z^2) \in \mathcal{O}[[Z]]$ such that*

$$-(x(Z), y(Z)) = (x(i(Z)), y(i(Z)))\,.$$

3. *Let $\phi \in \mathrm{End}_K(E)$. Then there exists a power series $\phi(Z) \in Z\mathcal{O}[[Z]]$ such that*

$$\phi(x(Z), y(Z)) = (x(\phi(Z)), y(\phi(Z)))\,.$$

Proof. For (1) and (2) see [Sil09][p. 119,120]. For (3) one has to follow a similar argument than in (1) and (2) which uses the Proposition 1.2.1. □

The previous proposition contains the necessary information to define a formal group.

Definition 1.2.4. The formal group associated to the elliptic curve E/K, denoted by $\hat{E}$, is a formal group over the ring $\mathcal{O}$ with the formal group law $F(Z_1, Z_2) \in \mathcal{O}[[Z_1, Z_2]]$ of Proposition 1.2.3, that corresponds to addition of points.

Computing the expression of $F(Z_1, Z_2)$ and using the fact that it comes from the group law of an elliptic curve it is possible to verify that it satisfies the properties of the definition of a formal group (this includes using the formula of the inverse of a point to deduce the existence and uniqueness of the power series $i(T)$).

As a corollary of the previous proposition we can find morphisms of the fomal group $\hat{E}$.

Corollary 1.2.5. *For every $\phi \in \mathrm{End}_K(E)$ there is a morphism $\phi(Z) \in Z\mathcal{O}[[Z]]$ of the formal group $\hat{E}/\mathcal{O}$ satisfying*

$$\phi(x(Z), y(Z)) = (x(\phi(Z)), y(\phi(Z))).$$

Moreover the power series $\phi(Z)$ has the form $\phi(Z) = aZ + O(Z^2)$ with $a \in K$ satisfying that $\phi^*(\omega) = a\omega$ for any invariant differential ω of E.

Proof. The first part is Proposition 1.2.3 (3). The second part follows from Corollary 1.1.14 and the fact that

$$\omega(z) = \frac{dx(Z)}{2y(Z) + a_1 x(Z) + a_3}$$

is an invariant differential of the formal group $\hat{E}/\mathcal{O}$. □

Now, notice that we can produce points of the curve using the power series $x(Z), y(Z)$. Indeed, if we take $z \in \mathfrak{p}$ the power series $x(z), y(z)$ converge to elements of K because they have all coefficients in $\mathcal{O}$. Since $x(Z), y(Z)$ satisfy the Weierstrass equation so does the point $P = (x(z), y(z))$. Thus, we get a map

$$\mathfrak{p} \to E(K), \quad z \mapsto (x(z), y(z)). \tag{1.5}$$

Here, $\mathfrak{p}$ is just a set, but we can give it a group structure so that this map is a morphism. It should be clear that the structure that we need is precisely the one given in Proposition 1.2.3. This is precisely the group associated to the formal group $\hat{E}$.

Definition 1.2.6. The group associated to the formal group $\hat{E}/\mathcal{O}$ is denoted by $\hat{E}(\mathfrak{p})$. Therefore, is the set $\mathfrak{p}$ endowed with the group operations

$$z_1 \oplus z_2 = F(z_1, z_2), \quad \ominus z = i(z)$$

for any $z, z_1, z_2 \in \mathfrak{p}$.

We are interested in studying the morphism of (1.5). For example, if we find its image in $E(K)$, it will be possible to translate the structure of $\hat{E}(\mathfrak{p})$ found in the section of formal groups to its image in $E(K)$ (we will see that the map is injective). The reduction map introduced in the next section will give us the tools to achieve this goal.

1.3 Reduction modulo π

Let E be an elliptic curve defined over K, choose a Weierstrass model of the curve

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where the $a_i \in K$. Recall that the substition $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ for $u \in K$ leads to a Weierstrass equation with coefficients $u^i a_i$ so we may assume that $a_i \in \mathcal{O}$ for every i.

We can reduce the coefficients of the curve modulo π obtaining the equation of a curve over the residue field k. This curve depends a lot on the value of u we choose. For example, the previous substition changes the discriminant of the curve: $\Delta \mapsto u^{-12}\Delta$, so if we choose an element $u \in K$ with a very negative valuation we will obtain a singular curve over k. We are interested in defining a general way to do this choice of u such that, whenever is possible, we obtain an elliptic curve over k. This motivates the following definitions.

Definition 1.3.1. A Weierstrass equation for E is minimal if $a_i \in \mathcal{O}$ for all i and the valuation of the discriminant of this equation is minimal in the set of valuations of all Weierstrass equations with coefficients in $\mathcal{O}$.

Definition 1.3.2. Choose a minimal Weierstrass equation for E

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The reduction of E is a curve $\tilde{E}$ over k defined by the Weierstrass equation

$$y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6}$$

where $\tilde{a_i} \in k$ is the reduction of a_i modulo $\mathfrak{p}$ for every i.

As we already said, the curve $\tilde{E}$ may not be an elliptic curve since it can have discriminant equal to zero. However, in this case it is well known that it has at most one singular point and the set of nonsingular points, E_{ns}, has a simple group structure.

Definition 1.3.3. Let Δ be the discriminant of the minimal Weierstrass equation. Then:

- If $\Delta \in \mathcal{O}^\times$ then $\tilde{E}$ is nonsingular and we say that E has good reduction.
- If $\Delta \notin \mathcal{O}^\times$, then $\tilde{E}$ is singular. If in addition $\tilde{E}_{\text{ns}}(k) \cong k^\times$ we say that E has multiplicative reduction.

- If $\Delta \notin \mathcal{O}^\times$, then $\tilde{E}$ is singular. If in addition $\tilde{E}_{\text{ns}}(k) \cong k^+$ we say that E has additive reduction.

In the last two cases we also say that E has bad reduction. When E has multiplicative reduction then it has a node. If the slopes of the tangent line at the node are in k we say that that the reduction is split. Otherwise we say it is nonsplit.

Definition 1.3.4. We say that E has potential good reduction if there exists a finite extension K'/K such that E has good reduction over K'.

The next step is to define a reduction map which sends points of the curve E defined over K to points of the curve $\tilde{E}$ defined over k. To do it consider the corresponding projective curve E with points in $\mathbb{P}^2(K)$. Given $P \in E(K)$ with coordinates $P = [X, Y, Z]$ we can scale these coordinates to ensure $X, Y, Z \in \mathcal{O}$ and that at least one coordinate has valuation zero. Supposing that X, Y, Z satisify this conditions define

$$\tilde{P} = [X \mod \pi, Y \mod \pi, Z \mod \pi].$$

The fact that at least one coordinate of P has valuation zero ensures that $\tilde{P} \in \mathbb{P}^2(k)$. It is also clear that $\tilde{P}$ satisfies the equation of $\tilde{E}$.

Following this same procedure, we can define the reduction map for points P that are defined over L, a finite extension of K: since L is also a local field we just need to choose a uniformizer $\pi' \in L$ and proceed in the same way as we explained. The reduced point $\tilde{P}$ will be a point of the curve $\tilde{E}$ defined over a finite extension of k.

Definition 1.3.5. Define:

$$E_0(K) = \left\{ P \in E(K) \mid \tilde{P} \in \tilde{E}_{\text{ns}}(k) \right\},$$

$$E_1(K) = \left\{ P \in E(K) \mid \tilde{P} = \tilde{O} \right\}.$$

Proposition 1.3.6. *If E is defined by a minimal Weierstrass equation*

$$E_1(K) = \{P = (x, y) \in E(K) \mid v(x) < 0\} \cup \{O\} = \{P = (x, y) \in E(K) \mid v(y) < 0\} \cup \{O\}.$$

And if $O \neq (x, y) \in E_1(K)$ then $3v(x) = 2v(y) = -6r$ for some positive integer r.

Proof. If $P = (x, y) \neq O$ such that $P \in E_1(K)$ it is clear that $v(x)$ or $v(y)$ have to be negative. Suppose that $v(x) < 0$ and consider the minimal Weierstrass equation of E

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Since $v(a_i) \geq 0$, the valuation on the right hand side of the equality is $3v(x) < 0$. This implies that $v(y) < 0$ which leads to $3v(x) = 2v(y)$. The case $v(y) < 0$ is analogous. □

As we already said, the set of nonsingular points of a curve defined by a Weierstrass equation forms a group with the geometric group law. The next proposition says that the reduction map is a morphism between $E_0(K)$ and $\tilde{E}_{\text{ns}}(k)$ and therefore induces the following exact sequence

Proposition 1.3.7. *There is an exact sequence of abelian groups*

$$0 \to E_1(K) \to E_0(K) \to \tilde{E}_{\text{ns}}(k) \to 0.$$

Proof. We present only an outline. For the complete proof see Silverman [Sil09] Chapter VII Proposition 2.1.

Everything is clear except that the map

$$E_0(K) \to \tilde{E}_{\text{ns}}(k)$$

is a surjective morphism. The surjectivity follows from Hensel's Lemma and to prove that it is a morphism one can work directly with the definition of the geometric group law (intersecting lines) and reduce this equations modulo $\mathfrak{p}$ and see that they agree with the group law of $\tilde{E}_{\text{ns}}(k)$. □

Finally, there is also a notion of reducing an isogeny.

Definition 1.3.8. Suppose E_1, E_2 are elliptic curves defined over K with good reduction and let $\phi : E_1 \to E_2$ be an isogeny. Define $\tilde{\phi} : \tilde{E}(k) \to \tilde{E}(k)$ as

$$\tilde{\phi}\tilde{P} = \widetilde{\phi(P)}.$$

Remark 1.3.9. The surjectivity of the map $E(K) \to \tilde{E}(k)$ allows us to define $\tilde{\phi}$ for points $\tilde{P}$ with $P \in E(K)$. However, it is not easy to prove that $\tilde{\phi}$ is well defined. It is also true that the reduction map preserves degrees. For the proof of this last statement (assuming that the reduction map is well defined) see [Sil94] Chapter 2 Proposition 4.4.

1.4 Applications to the study $E_1(K)$ and the torsion subgroup of E/K

Let E be an elliptic curve defined over K. Choose a minimal Weierstrass equation for E and consider the formal group $\hat{E}$ defined over $\mathcal{O}$ as well as the group $\hat{E}(\mathfrak{p})$ attached to it. We use the preciding section to find the image of the map (1.5). Then we translate the structure of $\hat{E}(\mathfrak{p})$ to its image which will allow us to deduce properties about the points of E.

Proposition 1.4.1. *The following map is a group isomorphism*

$$\hat{E}(\mathfrak{p}) \to E_1(K), \quad z \mapsto (x(z), y(z))$$

where $x(Z), y(Z) \in \mathcal{O}[[Z]]$ *are the power series of* (1.3), (1.4). *Its inverse is*

$$E_1(K) \to \hat{E}(\mathfrak{p}), \quad (x, y) \mapsto -x/y.$$

Proof. As it was discussed in the end of Section 1.2, if $z \in \mathfrak{p}$, then $(x(z), y(z)) \in E(K)$ and the map is a morphism. Moreover, since $Z^2x(Z) \in \mathcal{O}[[Z]]^\times$ and $Z^3y(Z) \in \mathcal{O}[[Z]]^\times$, Proposition 1.3.6 ensures that $(x(z), y(z)) \in E_1(K)$. Therefore we have a well defined morphism. By looking at the construction of the power series $x(Z), y(Z)$ we have that $Z = -x(Z)/y(Z)$, hence

$$z \mapsto (x(z), y(z)) \mapsto -x/y$$

is the identity. Since this implies that $(x, y) \mapsto -x/y$ is surjective we are left to see that it is injective as well. Let $(x, y) \in E_1(K)$ and write this point in (z, w)-coordinates (recall that $z = -x/y$ and $w = -1/y$). The minimal Weierstrass equation of E can be expressed in terms of the (z, w)-coordinates

$$a_6w^3 + (a_4z + a_3)w^2 + (a_2z^2 + a_1z - 1)w + z^3 = 0.$$

To prove the injectivity of the map we need to see that for a given $z = -x/y$ there is at most one w such that (z, w) corresponds to a point of $E_1(K)$. Since $(x, y) \in E_1(K)$, Lemma 1.3.6 gives us the valuations of x and y, and from here we deduce that $v(w) = 3v(z) > 0$.

Now, using the Cardano relations, it is plain to see that for a fixed z with positive valuation, the degree three equation with variable w has at most one root satisfying that $v(w) = 3v(z)$ proving the desired injectivity. Indeed, if we denote by w_1, w_2, w_3 the roots of the equation and for the sake of contradiction we suppose that $v(w_1) = v(w_2) = 3v(z)$ we obtain

$$v(w_3) = -3v(z) - v(a_6)$$

and

$$0 < v(a_4z + a_3) = v\left(a_6(w_1 + w_2 + w_3)\right) = v(a_6) + v(w_3) = -3v(z)$$

which is a contradiction.

□

Now we can translate the structure of $\hat{E}(\mathfrak{p})$ to $E_1(K)$.

Corollary 1.4.2. *Suppose that* E *has good reduction over* K. *Every element of finite torsion in* $E_1(K)$ *has torsion a power of* p. *Moreover, if* $(p-1) > v(p)$, $E_1(K) \cong \mathfrak{p}\mathcal{O}$ *so it is torsion free.*

Proof. This is a consequence of $E_1(K) \cong \hat{E}(\mathfrak{p})$ proven in Proposition 1.4.1. Now, we just have to apply Corollary 1.1.9 for the first part and use Theorem 1.1.19 for the second one. □

Now we show some applications of the previous corollary. Recall the definition of torsion points.

Definition 1.4.3. Let E be an elliptic curve defined over a field F. Let $\phi \in \mathrm{End}(E)$. Define the ϕ-torsion points as

$$E[\phi] = \{P \in E(\bar{F}) : \phi P = 0\}.$$

We also define $E(F)[\phi] = E[\phi] \cap E(F)$.

Corollary 1.4.4. *Suppose that E has good reduction over K. Let $m \in \mathbb{Z}$ be an integer coprime to p. Then the reduction map restricted to the m-torsion points is injective, i.e.*

$$E(K)[m] \hookrightarrow \tilde{E}(k).$$

Proof. Let $P \in E(K)[m]$ such that $\tilde{P} = \tilde{O}$, i.e. $P \in E_1(K)$. Then P is a point of m-torsion in $E_1(K)$, since Corollary 1.4.2 implies that there are no nontrivial elements of order coprime to p we obtain that $P = O$. □

Proposition 1.4.5. *Suppose that E has good reduction over K. Let $\phi \in \mathrm{End}_K(E)$ such that its corresponding power series is $\phi(Z) = aZ + O(Z^2) \in \mathcal{O}[[Z]]$ with $a \in \mathcal{O}^\times$. If $P \in E(\bar{K})$ such that $\phi(P) \in E(K)$, then $K(P, E[\phi])/K$ is unramified.*

Proof. The extension $K(P, E[\phi])/K$ is Galois, so let I be its inertia subgroup. If $\sigma \in I$ and $R \in E(\bar{K})$ so that $\phi(R) \in E(K)$

$$\widetilde{R^\sigma - R} = \tilde{R}^{\tilde{\sigma}} - \tilde{R} = \tilde{O},$$

hence $R^\sigma - R \in E_1(K)$. In addition, since ϕ is defined over K

$$\phi(R^\sigma - R) = \phi(R)^\sigma - \phi(R) = 0.$$

But by Proposition 1.1.8 $\phi(Z)$ is an isomorphism of $\hat{E}(\mathfrak{p})$, hence ϕ is an isomorphism of $E_1(F)$ (Proposition 1.4.1), which implies that $R^\sigma = R$. Therefore I is trivial. □

Recall the definition of the Tate module.

Definition 1.4.6. Let $\ell \in \mathbb{Z}$ be a prime. For each $n \geq 1$ we have the natural map

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n].$$

The ℓ-adic Tate module of E is the group

$$T_\ell(E) = \varprojlim_n E[\ell^n],$$

where the inverse limit is taken with respect to the previous maps.

Corollary 1.4.7. *Let I be the inertia subgroup of G_K.*

1. *Suppose that E has good reduction at K. If $m \in \mathbb{Z}$ is an integer coprime to p, the extension $K(E[m])/K$ is unramified. Hence, I acts trivially on $T_\ell(E)$ for $\ell \neq p$.*

2. *Suppose that E has potential good reduction over K. Then I acts on $T_\ell(E)$ through a finite quotient.*

Proof. 1. Apply Proposition 1.4.5 with $\phi = [m]$.

2. Let K' be a finite extension of K where E has good reduction. Denote by I' the inertia group of $G_{K'}$. By (1), I' acts trivially on $T_\ell(E)$, therefore I acts on $T_\ell(E)$ through the quotient I/I' which is the inertia group of K'/K and hence finite.

□

There is a converse to this statement, we give the theorem without the proof because we have not presented all the necessary tools to prove it.

Theorem 1.4.8 (Criterion of Néron–Ogg–Shafarevich)**.** *Let I be the inertia subgroup of G_K.*

1. *If I acts trivally on $T_\ell(E)$ for some $\ell \neq p$, E has good reduction over K.*

2. *If $T_\ell(E)^I \neq 0$ for some $\ell \neq p$, E has good or multiplicative reduction.*

Proof. See [Sil09] Chapter VII Theorem 7.1 for (1) and [Rub99] Theorem 3.19 for (2). □

Chapter 2

Elliptic curves with complex multiplication

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}$. In this chapter we study the properties of elliptic curves with complex multiplication. Using the so called Main Theorem of complex multiplication we will be able to study the extensions of K adjoining torsion points of the curve and their Galois group. For simplicity we restrict to the case where the curve has complex multiplication by the ring of integers $\mathcal{O}$.

In the first section there is a quick review of the basic facts about elliptic curves defined over $\mathbb{C}$. For a more detailed exposition with proofs see [Sil09] Chapter VI. The main references for the rest of the chapter are [Sil94] Chapter II and [Rub99] Chapter 5.

2.1 Review of elliptic curves over $\mathbb{C}$

Let E be an elliptic curve defined over $\mathbb{C}$. In this case it is possible to study the group of points of E (in particular the torsion points) from an analytic point of view. This will allow us to give a simple description of the isogenies between two elliptic curves defined over $\mathbb{C}$ and to find the possibilities for the endomorphism ring of E. In doing this last thing we will give the definition of a curve with complex multiplication. Since the goal of this section is to do a quick review of these basic statements there will not be proofs of them.

The main result of the section is that we have a correspondence between elliptic curves $E/\mathbb{C}$ modulo isomorphism and lattices $L \subset \mathbb{C}$ modulo homothety. This correspondence comes from the analytic isomorphism between $E(\mathbb{C})$ and the torus $\mathbb{C}/L$.

Definition 2.1.1. A lattice $L \subset \mathbb{C}$ is a discrete subgroup of $\mathbb{C}$ that contains an $\mathbb{R}$-basis of $\mathbb{C}$. Thus, there exists $\omega_1, \omega_2 \in \mathbb{C}$, $\mathbb{R}$-basis of $\mathbb{C}$ such that

$$L = \{n_1\omega_1 + n_2\omega_2 \mid n_1, n_2 \in \mathbb{Z}\}.$$

In order to explain the relation between elliptic curves and lattices we need to introduce the following definitions.

Definition 2.1.2. Let $L \subset \mathbb{C}$ be a lattice.

1. The Weierstrass $\wp$-function is

$$\wp(z, L) = \frac{1}{z^2} + \sum_{0 \neq \omega \in L} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

2. For a positive integer k, the Eisenstein series of weight $2k$ is

$$G_{2k}(L) = \sum_{0 \neq \omega \in L} \omega^{-2k}.$$

Now, the following theorem precises what we have said so far.

Theorem 2.1.3. *1. Let L be a lattice. Consider its associated curve defined over $\mathbb{C}$*

$$E_L : y^2 = x^3 - 15G_4(L)x - 35G_6(L).$$

Then E_L is an elliptic curve and it is analytically isomorphic to $\mathbb{C}/L$ via the map

$$f : \mathbb{C}/L \to E_L(\mathbb{C}), \quad z \mapsto (\wp(z, L), \wp'(z, L)/2)$$

where 0 goes to the point at infinity of E.

2. Coversely, given $E/\mathbb{C}$ elliptic curve with equation $y^2 = x^3 + ax + b$ there is a unique lattice $L \subset \mathbb{C}$ such that $a = -15G_4(L), b = -35G_6(L)$ and the map f of (1) gives an analytic isomorphism from $\mathbb{C}/L$ to E. Moreover, if ω_E is the normalized invariant differential of E, f identifies ω_E with dz.

The next step is to study how the isogenies between curves translate to analytic maps between the corresponding torus $\mathbb{C}/L$.

Theorem 2.1.4. *Let E_1, E_2 be elliptic curves over $\mathbb{C}$ with corresponding lattices L_1, L_2. Let $f_i : \mathbb{C}/L_i \xrightarrow{\sim} E_i$ be the corresponding isomorphisms of Theorem 2.1.3 for $i = 1, 2$. Then we have the bijection*

$$\{\alpha \in \mathbb{C} \mid \alpha L_1 \subset L_2\} \to \{\textit{isogenies from } E_1 \textit{ to } E_2\}, \quad \alpha \mapsto \phi_\alpha,$$

where ϕ_α is defined such that the following diagram is commutative

$$\begin{array}{ccc} \mathbb{C}/L_1 & \xrightarrow{\cdot\alpha} & \mathbb{C}/L_2 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} \\ E_1 & \xrightarrow{\phi_\alpha} & E_2. \end{array}$$

So an isogeny between two curves E_1 and E_2 translates to the map multiplication by α. This leads to the following corollary.

Corollary 2.1.5. *Let E_1, E_2 be two elliptic curves with corresponding lattices L_1, L_2. Then, E_1, E_2 are isomorphic if and only if L_1 and L_2 are homothetic.*

Remark 2.1.6. In the case that $E_1 = E_2$ the bijection from Proposition 2.1.4

$$\{\alpha \in \mathbb{C} \mid \alpha L \subset L\} \to \mathrm{End}(E)$$

is an isomorphism of rings.

This expression for $\mathrm{End}(E)$ allow us to determine all the possibilities for this ring.

Proposition 2.1.7. *Let $E/\mathbb{C}$ be an elliptic curve. Let L be its associated lattice with generators $\omega_1, \omega_2 \in \mathbb{C}$. Then, exactly one of the following is true:*

1. *The ring $\{\alpha \in \mathbb{C} \mid \alpha L \subset L\} = \mathbb{Z}$,*
2. *The field $\mathbb{Q}(\omega_2/\omega_1)$ is an imaginary quadratic field and $\{\alpha \in \mathbb{C} \mid \alpha L \subset L\} = \mathscr{o}$, where $\mathscr{o}$ is an order $\mathbb{Q}(\omega_2/\omega_1)$.*

Therefore the ring $\mathrm{End}(E)$ is either isomorphic to $\mathbb{Z}$ or isomorphic to an order in $\mathbb{Q}(\omega_2/\omega_1)$.

Definition 2.1.8. Let E be an elliptic curve defined over $\mathbb{C}$. We say that E has complex multiplication if $\mathrm{End}(E)$ is isomorphic to an order in an imaginary quadratic field.

The theory we just explained can be applied to study properties about the endomorphism ring of a curve and its torsion points. Recall the definition of the torsion points of an endomorphism.

Suppose that E is defined over $\mathbb{C}$ and it does not have complex multiplication (Case (1) of Proposition 2.1.7). Then, the structure of $\mathrm{End}(E)$ and its torsion points is quite simple since every endomorphism corresponds to add a point m times for some integer $m \in \mathbb{Z}$. In the following example we can see structure of $E[m]$.

Example 2.1.9. Let $E/\mathbb{C}$ be an elliptic curve and $m \in \mathbb{Z}$. By Theorem 2.1.3 (2) $E(\mathbb{C}) \cong \mathbb{C}/L$ for some lattice L. Then

$$E[m] \cong (\mathbb{C}/L)\,[m] = \{z \in \mathbb{C}/L \mid mz \in L\} = m^{-1}L/L \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

where we used the structure of a lattice of Definition 2.1.2 for the last isomorphism.

On the other hand, when E is an elliptic curve defined over $\mathbb{C}$ with complex multiplication there are more options for $\phi \in \mathrm{End}(E)$ than just multiplication-by-m. Therefore, the structure of $\mathrm{End}(E)$ and its torsion points is not that simple. The goal of the next section is to use the previous theory to study them.

2.2 Elliptic curves with complex multiplication over $\mathbb{C}$

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}$. Let E be an elliptic curve defined over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$. The aim of this section is to study the endomorphisms of E. This means finding an identification of the ring $\mathrm{End}(E)$ with $\mathcal{O}$. Then, we will find the structure of the torsion points of an endomorphism of E. However, in order to justify that the following statements are nontrivial we will start by recalling that there exists a curve with the properties of E.

Proposition 2.2.1. *There exists a curve $E_{\mathcal{O}}$ defined over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$.*

Proof. It is plain to check that $L = \mathcal{O} \subset \mathbb{C}$ is a lattice. Following Theorem 2.1.3 (1) there exists $E_{\mathcal{O}}$ such that $\mathbb{C}/L \cong E_{\mathcal{O}}$. It is easy to check that

$$\mathcal{O} = \{\alpha \in \mathbb{C} : \alpha\mathcal{O} \subset \mathcal{O}\}.$$

so the result follows from Remark 2.1.6. □

Remark 2.2.2. In fact, it is not hard to see the number (up to isomorphism) of elliptic curves defined over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$ is precisely the class number of K (see [Sil94] Chapter II Proposition 1.2).

Proposition 2.2.3. *There exists a unique ring isomorphism $[\ ] : \mathcal{O} \xrightarrow{\sim} \mathrm{End}(E)$ satisfying that, for any invariant differential ω on E,*

$$[\alpha]^*\omega = \alpha\omega$$

for all $\alpha \in \mathcal{O}$.

Proof. By Theorem 2.1.3 (2) there exists a lattice L so that $E = E_L$ and let $f : \mathbb{C}/L \xrightarrow{\sim} E$ be the analytic isomorphism. Using Proposition 2.1.7 we have that $\mathcal{O} = \{\alpha \in \mathbb{C} \mid \alpha L \subset L\}$. Define the map $[\ ]$ as

$$[\alpha] := \phi_\alpha,$$

where ϕ_α is the isogeny defined in Theorem 2.1.4. Hence we have that

$$\begin{array}{ccc} \mathbb{C}/L & \xrightarrow{\cdot\alpha} & \mathbb{C}/L \\ \downarrow f & & \downarrow f \\ E & \xrightarrow{[\alpha]} & E \end{array}$$

is commutative. Now let ω be an invariant differential of E, since the space of invariant differentials is one dimensional and f identifies ω_E with dz we have $f^*(\omega) = c\,dz$ for some constant c. Therefore

$$[\alpha]^*(\omega) = f^* \circ (\cdot\alpha)^* \circ \left(f^{-1}\right)^* (\omega) = f^* \circ (\cdot\alpha)^*(c^{-1}\,dz) = f^*(c^{-1}\alpha\,dz) = \alpha\omega.$$

The uniqueness of the map follows from this last equation, since we get that the endomorphism $[\alpha]$ has to correspond to the map multiplication by α. □

The following lemma will be used in the next sections in order to study the field of definition of an endomorphism.

Lemma 2.2.4. *For every $\sigma \in \mathrm{Aut}(\mathbb{C})$ and $\alpha \in \mathcal{O} \cong \mathrm{End}(E)$*

$$[\alpha]_E^\sigma = [\alpha^\sigma]_{E^\sigma}$$

Remark 2.2.5. In order to explain and prove this Proposition recall the action of $\sigma \in \mathrm{Aut}(\mathbb{C})$ on the following objects. If $\phi \in \mathrm{End}(E)$, σ acts as

$$\phi^\sigma : E^\sigma \to E^\sigma, \quad \phi^\sigma = \sigma \circ \phi \circ \sigma^{-1}.$$

Similarly, if $f \in \bar{K}(E)$ the function field, σ also acts by conjugation. Now, we can make explicit the action of σ on differentials ω as

$$(\omega)^\sigma = \left(\sum_{i=1}^{n} f_i\,dx_i\right)^\sigma = \sum_{i=1}^{n} f_i^\sigma\,dx_i^\sigma.$$

Where x_i are also elements of the function field. In the particular case where the x_i are coordinate functions of E, it is easy to check that x_i^σ goes to the corresponding x_i coordinate function of E^σ. Note that the action by conjugation of σ can also

be thought as applying σ to the expressions of ϕ, f or ω (in case that the x_i are coordinate functions).

From these observations, if

$$\omega_E = \frac{dx}{2y + a_1 x + a_3}$$

is an invariant differential of E, it is clear that ω_E^σ is an invariant differential of E^σ with expression

$$\omega_E^\sigma = \frac{dx}{2y + a_1^\sigma x + a_3^\sigma}.$$

Proof. We will use Proposition 2.1.3 that characterizes the endomorphisms with the map [ ]. Let ω be an invariant differential of E, then ω^σ is an invariant differential of E^σ. Note that by Proposition 2.1.3

$$[\alpha^\sigma]_{E^\sigma}^* \omega^\sigma = \alpha^\sigma \omega^\sigma.$$

On the other hand, using the expressions from Remark 2.2.5, one can compute

$$\left([\alpha]_E^\sigma\right)^* \omega^\sigma = \left([\alpha]^* \omega\right)^\sigma = (\alpha\omega)^\sigma .$$

By the proof of Proposition 2.1.3 both endomorphisms correspond to multiplication by α^σ, so they are the same.

□

We proceed to study the torsion points of E.

Definition 2.2.6. Let $\mathfrak{a}$ be an integral ideal of $\mathcal{O}$. Define the group of $\mathfrak{a}$-torsion points of E as

$$E[\mathfrak{a}] = \{P \in E \mid [\alpha]P = O \text{ for all } \alpha \in \mathfrak{a}\},$$

where [ ] is the map from Proposition 2.2.3. From Definition 1.4.3 we can write

$$E[\mathfrak{a}] = \cap_{\alpha \in \mathfrak{a}} E[\alpha].$$

Define $E[\mathfrak{a}^\infty] = \cup_n E[\mathfrak{a}^n]$.

Proposition 2.2.7. *Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$. Then $E[\mathfrak{a}]$ is a free $\mathcal{O}/\mathfrak{a}$-module of rank 1.*

Proof. Let L be the associated lattice of E. We can scale this lattice so that it is a fractional ideal of K. Indeed, if ω_1, ω_2 are generators of L, by Proposition 2.1.7 we see that $\frac{1}{\omega_1} L \subset K = \mathbb{Q}(\omega_2/\omega_1)$ and since L is a lattice and E has complex multiplication

by $\mathcal{O}$ we have that $\frac{1}{\omega_1}L$ is an $\mathcal{O}$-module of rank 2 contained in K and therefore, a fractional ideal of K. Hence, we may assume that L is a fractional ideal.

Fix an analytic isomorphism $\xi : \mathbb{C}/L \xrightarrow{\sim} E$. Then if $P = \xi(z) \in E$, $[\alpha]P = \xi(\alpha z)$ by Proposition 2.1.3. Thus

$$E[\mathfrak{a}] = \{P \in E \mid [\alpha]P = O \text{ for all } \alpha \in \mathfrak{a}\} \cong \{z \in \mathbb{C}/L \mid \alpha z \in L \text{ for all } \alpha \in \mathfrak{a}\}.$$

This is an isomorphism of $\mathcal{O}$-modules because it is an isomorphism of groups and multiplication by $\alpha \in \mathcal{O}$ in $\mathbb{C}/L$ corresponds to apply $[\alpha]$ in E. Moreover, $\mathcal{O}$ is acting on $E[\mathfrak{a}]$ so multiplication by $\mathcal{O}$ factors through $\mathcal{O}/\mathfrak{a}$. Thus, we obtain an isomorphism of $\mathcal{O}/\mathfrak{a}$-modules. Now

$$\{z \in \mathbb{C}/L \mid \alpha z \in L \text{ for all } \alpha \in \mathfrak{a}\} = \{z \in \mathbb{C}/L \mid \mathfrak{a}z \in L\} = \mathfrak{a}^{-1}L/L.$$

The following lemma applied to the case $\mathfrak{b} = \mathfrak{a}^{-1}L$ completes the proof. □

Lemma 2.2.8. *Let $\mathfrak{a} \subset \mathcal{O}$ be an integral ideal and $\mathfrak{b}$ a fractional ideal of K. Then $\mathfrak{b}/\mathfrak{a}\mathfrak{b}$ is a free $\mathcal{O}/\mathfrak{a}$-module of rank 1. In particular $\#E[\mathfrak{a}] = \mathrm{N}_{K/\mathbb{Q}}\mathfrak{a}$.*

Proof. It is possible to generalize the Chinese Remainder Theorem to obtain the following group isomorphism (the proof works in the same way that for the case $\mathfrak{b} = \mathcal{O}$)

$$\mathfrak{b}/\mathfrak{a}\mathfrak{b} \xrightarrow{\sim} \prod_{i=1}^{k} \mathfrak{b}/\mathfrak{p}_i^{e_i}\mathfrak{b}, \quad [x] \mapsto ([x]_1, \ldots, [x]_k)$$

where $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$. In fact, this isomorphism respects multiplication by $\mathcal{O}/\mathfrak{a}$, so it is a $\mathcal{O}/\mathfrak{a}$-module isomorphism.

Observe that the action of $\mathcal{O}/\mathfrak{a}$ on the component $\mathfrak{b}/\mathfrak{p}_i^{ei}\mathfrak{b}$ factors through $\mathcal{O}/\mathfrak{p}_i^{e_i}$. Therefore, if we prove that $\mathfrak{b}/\mathfrak{p}_i^{e_i}\mathfrak{b}$ is a free $\mathcal{O}/\mathfrak{p}_i^{e_i}$-module of rank 1 the desired result will follow from the Chinese Remainder Theorem applied to the ring $\mathcal{O}/\mathfrak{a}$.

To prove this last statement we will apply Nakayama's Lemma ([AM69], Proposition 2.8) to the following module

$$M = \mathfrak{b}/\mathfrak{p}_i^{e_i}\mathfrak{b}, \quad R = \mathcal{O}/\mathfrak{p}_i^{e_i}.$$

Note that M is an R-module and R is a local ring with maximal ideal $\mathfrak{m} = \mathfrak{p}_i/\mathfrak{p}_i^{e_i}$. Consider $M/\mathfrak{m}M \cong \mathfrak{b}/\mathfrak{p}\mathfrak{b}$ as a $R/\mathfrak{m} \cong \mathcal{O}/\mathfrak{p}$-vector space. This is a 1 dimensional vector space. Indeed, $\mathfrak{b} \neq \mathfrak{p}\mathfrak{b}$ so the dimension is at least one, but any two elements of $\mathfrak{b}$ are $\mathcal{O}$-linearly dependent, so reducing modulo $\mathfrak{p}$, any two elements of $\mathfrak{b}/\mathfrak{p}\mathfrak{b}$ are $\mathcal{O}/\mathfrak{p}$-linearly dependent. Therefore, Nakayama's Lemma tells us that M is generated by one element as an R-module.

To prove that the module is free let $[e] \in M$ be a R-generator of M and suppose that there exists $[k] \in R$ such that $[k][e] = 0$. In other words, $ke \in \mathfrak{p}_i^{e_i}\mathfrak{b}$. But since e is a generator of M it is easy to see that $k\mathfrak{b} \subset \mathfrak{p}_i^{e_i}\mathfrak{b}$ and hence $k \in \mathfrak{p}_i^{e_i}$. So $[k] = 0$ in R and we are done. □

2.3 Torsion subgroups

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}$. Let F be a field of characteristic 0 that can be injected in $\mathbb{C}$. Consider an elliptic curve E defined over F with complex multiplication by $\mathcal{O}$. Injecting $F \hookrightarrow \mathbb{C}$, we can apply the results for elliptic curves defined over $\mathbb{C}$ of the previous two sections to the curve E (see The Lefschetz Principle, [Sil09] Chapter VI Section 6).

Proposition 2.3.1. *Suppose that F is subfield of $\mathbb{C}$. Then every endomorphism of E is defined over the composition KF.*

Proof. Let $\sigma \in \mathrm{Aut}(\mathbb{C}/KF)$ and pick any endomorphism $[\alpha]_E$ whith $\alpha \in \mathcal{O}$. Lemma 2.2.4 says

$$[\alpha]_E^\sigma = [\alpha^\sigma]_{E^\sigma}.$$

But $E = E^\sigma$ because σ fixes F. Using that σ also fixes K we conclude the proof

$$[\alpha^\sigma]_E = [\alpha]_E.$$

□

Proposition 2.3.2. *Suppose that F contains K. Let $\mathfrak{a}$ be an integral ideal of K. Then, the action of the Galois group $\mathrm{Gal}(F(E[\mathfrak{a}])/F)$ on the $\mathfrak{a}$-torsion points induces an injection*

$$\mathrm{Gal}(F(E[\mathfrak{a}])/F) \hookrightarrow (\mathcal{O}/\mathfrak{a})^\times.$$

In particular, $F(E[\mathfrak{a}])$ is an abelian extension of F.

Proof. It is clear that $F(E[\mathfrak{a}])/F$ is Galois. Every $\sigma \in \mathrm{Gal}(F(E[\mathfrak{a}])/F)$ induces an $\mathcal{O}/\mathfrak{a}$-automorphism of $E[\mathfrak{a}]$

$$\rho_\sigma : E[\mathfrak{a}] \to E[\mathfrak{a}], \quad P \mapsto P^\sigma.$$

To prove it, note that ρ_σ is clearly bijective and linear with respect to addition so we only need to see that it is linear with respect to multiplication by $\mathcal{O}/\mathfrak{a}$. This follows from the fact that every $[\alpha] \in \mathrm{End}(E)$ is defined over F (injecting $F \hookrightarrow \mathbb{C}$ we can apply Proposition 2.3.1) and hence

$$\rho_\sigma([\alpha]P) = ([\alpha]P)^\sigma = [\alpha]P^\sigma = [\alpha]\rho_\sigma(P).$$

Therefore, we have following morphism

$$\rho : \mathrm{Gal}(F(E[\mathfrak{a}])/F) \to \mathrm{Aut}_{\mathcal{O}/\mathfrak{a}}(E[\mathfrak{a}]), \quad \sigma \mapsto \rho_\sigma.$$

which is clearly injective. Indeed, if $\rho_\sigma(P) = P$ for every $P \in E[\mathfrak{a}]$, σ fixes $E[\mathfrak{a}]$, i.e., σ is the identity in $\mathrm{Gal}(F(E[\mathfrak{a}])/F)$.

Finally, Lemma 2.2.7 proves that $E[\mathfrak{a}]$ is a free $\mathcal{O}/\mathfrak{a}$-module of rank one, therefore $\mathrm{Aut}_{\mathcal{O}/\mathfrak{a}}(E[\mathfrak{a}])$ correspond to multiplication by an element of $(\mathcal{O}/\mathfrak{a})^\times$ and we are done. □

Corollary 2.3.3. *Let p be a rational prime. Then*

$$\mathrm{Gal}(F(E[p^\infty])/F) \hookrightarrow (\mathcal{O} \otimes \mathbb{Z}_p)^\times .$$

Similarly,

$$\mathrm{Gal}\left(F(E[p^\infty])/F(E[p])\right) \hookrightarrow (1 + p\mathcal{O}) \otimes \mathbb{Z}_p.$$

Proof. For every $n \geq 1$, there is an injection:

$$\mathrm{Gal}(F(E[p^n])/F) \hookrightarrow (\mathcal{O}/p^n\mathcal{O})^\times .$$

Taking the inverse limit with respect to n leads to the first assertion.

For the second one, note that the previous injection restricts to

$$\mathrm{Gal}(F(E[p^n])/F(E[p])) \to \left\{x \in (\mathcal{O}/p^n\mathcal{O})^\times : x \equiv 1 \mod p\mathcal{O}\right\}$$

since the automorphisms of $E[p^n] \cong \mathcal{O}/p^n\mathcal{O}$ that fix the p-torsion are precisely multiplication by an element $x \equiv 1 \mod p\mathcal{O}$. Again, taking the inverse limit in both sides we are done. □

Theorem 2.3.4. *Suppose that F is a finite extension of $\mathbb{Q}_\ell$ containing K, where ℓ is a rational prime.*

1. *E has potential good reduction.*
2. *Let $\mathfrak{p}$ be a prime of K not dividing ℓ. Let $m \in \mathbb{Z}$ such that $1 + \mathfrak{p}^m\mathcal{O}_\mathfrak{p}$ is torsion free. Then, E has good reduction over $F(E[\mathfrak{p}^m])$.*

Proof. 1. Let $p > 3$ be a rational prime, $p \neq \ell$, which remains prime in K (this exists by the Cebotarev Theorem or, more elementarily, by the study of which primes of an imaginary quadratic field are inert). We will prove that E has good reduction over $F(E[p])$.

Under this conditions, Corollary 2.3.3 says

$$\mathrm{Gal}(F(E[p^\infty])/F(E[p])) \hookrightarrow U^{(1)}$$

with $U^{(1)} \subset \mathcal{O}_p^\times$ the 1st higher unit group. Since $p > 3$, the p-adic logarithm map gives the isomorphism $U^{(1)} \xrightarrow{\sim} \mathcal{O}_p \cong \mathbb{Z}_p^2$. Hence

$$\mathrm{Gal}(F(E[p^\infty])/F(E[p])) \hookrightarrow \mathbb{Z}_p^2.$$

But $\mathrm{Gal}(F(E[p^\infty])/F(E[p]))$ is compact, so its image in $\mathbb{Z}_p^2$ is compact too, and therefore closed. Since the closed subgroups of $\mathbb{Z}_p$ are either 0 or isomorphic to $\mathbb{Z}_p$ we conclude

$$\mathrm{Gal}(F(E[p^\infty])/F(E[p])) \xrightarrow{\sim} \mathbb{Z}_p^d$$

with $d = 1$ or 2. Such an extension with this Galois group is unramfied. Indeed, if we denote $\mathcal{O}_{F(E[p])}$ the ring of integers of $F(E[p])$, the local Artin map gives a surjective morphism

$$\mathcal{O}_{F(E[p])}^\times \to I,$$

where I is the inertia subgroup of $\mathrm{Gal}(F(E[p^\infty])/F)$. On one hand we have that $\mathcal{O}_{F(E[p])} \cong \omega \times \mathbb{Z}_l^r$, where ω is a finite group and $r \geq 1$ an integer. On the other hand $I \cong \mathbb{Z}_p^i$ for $i \leq d$ (since it is a closed subgroup of $\mathbb{Z}_p^d$). It is plain to conclude that $I = 0$ as desired. By the criterion of Néron-Ogg-Shafarevich (Theorem 1.4.8 (1)), E has good reduction over $F(E[p])$.

2. Let p be the rational prime below $\mathfrak{p}$, $F_\infty = F(E[\mathfrak{p}^\infty])$ and $F_m = F(E[\mathfrak{p}^m])$. Following the reasoning done in the proof of Corollary 2.3.3 one sees that

$$\mathrm{Gal}(F_\infty/F_m) \hookrightarrow 1 + \mathfrak{p}^m\mathcal{O}_\mathfrak{p}.$$

On the other hand, (1) implies that E has potential good reduction over F_m, so by Corollary 1.4.7 (2), I_{F_m}, the inertia subgroup of G_{F_m}, acts on $T_p(E)$ through a finite quotient. Since $E[\mathfrak{p}^n] \subset E[p^n]$ for every n, I_{F_m} acts on F_∞ through a finite quotient too. Therefore, the inertia subgroup of $\mathrm{Gal}(F_\infty/F_m)$ has to be finite, but, by hypothesis, the only finite subgroup of $1 + \mathfrak{p}^m\mathcal{O}_\mathfrak{p}$ is trivial.

We have seen that F_∞/F_m is fixed by I_{F_m} and combining this with $E[\mathfrak{p}^n] \subset E[p^n]$ for every n leads to $T_p(E)^{I_{F_m}} \neq 0$. By the criterion of Néron–Ogg–Shafarevich (Theorem 1.4.8 (2)) E has either good or multiplicative reduction. It is well known that since E already has potential good reduction the only possibility is that E has good reduction and we are done.

□

2.4 Main Theorem and algebraicity of CM elliptic curves

Recall K is an imaginary quadratic field with ring of integers $\mathcal{O}$. Let E be an elliptic curve defined over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$.

We begin this chapter by proving the Main Theorem of complex multiplication. It gives an analytic description of how an element of $\mathrm{Aut}(\mathbb{C}/K)$ acts on the torsion points of E. There is an analog (and simpler) version of this theorem that describes the action of an automorphism $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ on the roots of unity $\zeta \in \mathbb{C}^\times$. Note that in this last case the roots of unity correspond to torsion points of $\mathbb{C}^\times$. The proof of the main theorem of complex multiplication can be found in [Sil94] Chapter II Section 8.

After that, we use the Main Theorem to see that there exists a curve E' which is $\mathbb{C}$-isomorphic to E defined over the Hilbert class field of K. This is remarkable since for an elliptic curve without CM it is not true in general that it is isomorphic to a curve defined over an algebraic extension of $\mathbb{Q}$.

The Main Theorem of complex multiplication will have a crucial role for the rest of the chapter, since it will allow us to study extensions of K obtained by adjoining torsion points via a Hecke character (which we will define in the next section).

From a given number field F with ring of integer $\mathcal{O}_F$ we will use the following notation. For every place v we denote by F_v the completion of v with respect to the corresponding norm. If $\mathfrak{a}$ is an ideal of F, we denote by $\mathfrak{a}_v$ the corresponding ideal in F_v. Denote by $\mathbb{A}_F^\times$ the idele group. Their elements are sequences $(x_v) \in \prod_v F_v^\times$ where the product is over all places (finite and infinite) such that $x_v \in \mathcal{O}_{F,v}^\times$ for all but finitely many v. Recall $\mathbb{A}_F^\times$ has a group structure and a natural topology. We will denote by $[\cdot, F] : \mathbb{A}_F^\times \to \mathrm{Gal}(F^{\mathrm{ab}}/F)$ the global Artin map, where F^{ab} is the maximal abelian extension of F and by $[\cdot, F_v^{\mathrm{ab}}/F_v] : F_v^\times \to \mathrm{Gal}(F_v^{\mathrm{ab}}/F_v)$ the local Artin map although we will not need it in this section.

We start defining the analytic maps that will allow us to describe the action of an automorphism $\sigma \in \mathrm{Aut}(\mathbb{C})$.

Proposition 2.4.1. *Let $\mathfrak{a}$ be a fractional ideal of K. There is the following isomorphism*

$$K/\mathfrak{a} \cong \bigoplus_{\mathfrak{p}} K_\mathfrak{p}/\mathfrak{a}_\mathfrak{p}$$

where the sum is over the finite prime ideals $\mathcal{O}$.

Proof. See Silverman [Sil94] Chapter II Lemma 8.1. □

Definition 2.4.2. Let $x = (x_\mathfrak{p}) \in \mathbb{A}_K^\times$ and denote by (x) its corresponding finite ideal.

1. For each finite $\mathfrak{p}$ define the multiplication by $x_\mathfrak{p}$ map

$$\cdot x_\mathfrak{p} : K_\mathfrak{p}/\mathfrak{a}_\mathfrak{p} \to K_\mathfrak{p}/x_\mathfrak{p}\mathfrak{a}_\mathfrak{p}, \quad y \mapsto x_\mathfrak{p} y.$$

2. Using the decomposition of Proposition 2.4.1 define the map $\cdot x$ (sometimes we will denote it only by x) via the following commutative diagram

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\cdot x} & K/(x)\mathfrak{a} \\ \downarrow\wr & & \downarrow\wr \\ \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}} & \xrightarrow{(\cdot x_{\mathfrak{p}})} & \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}/x_{\mathfrak{p}}\mathfrak{a}_{\mathfrak{p}} \end{array}$$

Remark 2.4.3. An elliptic curve $E/\mathbb{C}$ with complex multiplication by $\mathcal{O}$ is analytically isomorphic to $\mathbb{C}/\mathfrak{a}$ where the lattice $\mathfrak{a}$ is a fractional ideal of K. Using this isomorphism we see that the torsion points E_{tors} correspond to $K/\mathfrak{a} \subset \mathbb{C}/\mathfrak{a}$. Thus, the map $\cdot x$ can be seen as a map between the torsion points of two elliptic curves with lattices $\mathfrak{a}$ and $(x)\mathfrak{a}$.

Now we can state the Main Theorem.

Theorem 2.4.4 (Main Theorem of complex multiplication)**.** *Let $\mathfrak{a}$ be a fractional ideal of $\mathfrak{a}$ such that*

$$f : \mathbb{C}/\mathfrak{a} \xrightarrow{\sim} E(\mathbb{C}).$$

is an analytic isomorphism. Fix $\sigma \in \text{Aut}(\mathbb{C}/K)$ and an idele $x \in \mathbb{A}_K^\times$ such that $[x, K] = \sigma|_{K^{ab}}$. Then, there exists a unique analytical isomorphism

$$f' : \mathbb{C}/x^{-1}\mathfrak{a} \xrightarrow{\sim} E^\sigma(\mathbb{C}).$$

such that the following diagram commutes

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{f} & E(\mathbb{C}) \\ \downarrow{\scriptstyle x^{-1}} & & \downarrow{\scriptstyle \sigma} \\ K/x^{-1}\mathfrak{a} & \xrightarrow{f'} & E^\sigma(\mathbb{C}). \end{array}$$

Proof. See Silverman [Sil94] Chapter II Theorem 8.2. □

We proceed to use this theorem to relate the j-invariant of E, $j(E)$, with the Hilbert class field of E. This can be proven without using the Main Theorem explicitly, see [Sil94] Chapter II Section 4. For example, the fact that $j(E)$ is an algebraic number is more elementary. We will not present these proofs for space reasons.

Proposition 2.4.5. *The extension $K(j(E))$ is the Hilbert class field of K.*

Proof. Choose a fractional ideal $\mathfrak{a}$ such that $E \cong \mathbb{C}/\mathfrak{a}$.

Let $x \in \mathbb{A}_K^\times$. Recall that $\mathbb{C}/\mathfrak{a} \cong \mathbb{C}/x^{-1}\mathfrak{a}$ if and only if the lattices $\mathfrak{a}$ and $x^{-1}\mathfrak{a}$ are homothetic. By the Main Theorem

$$j(E) = j(E)^{[x,K]} \iff E \cong E^{[x,K]} \iff \mathbb{C}/\mathfrak{a} \cong \mathbb{C}/x^{-1}\mathfrak{a}.$$

Hece the lattices are homothetic, i.e. there exists $\lambda \in K^\times$ such that

$$\lambda\mathfrak{a} = x^{-1}\mathfrak{a} \iff x \in K^\times \prod_{v|\infty} K_v^\times \prod_{v\nmid\infty} \mathcal{O}_v^\times$$

and by class field theory the automorphisms $[x, K]$ with x in this subgroup are precisely the ones fixing the Hilbert class field. □

Corollary 2.4.6. *There exists an elliptic curve E' defined over the Hilbert class field of K with complex multiplication by $\mathcal{O}$ which is $\mathbb{C}$-isomorphic to E.*

Proof. This follows from Proposition 2.2.1 and the fact that E is isomorphic (and the isomorphism is defined over $\mathbb{C}$) to a curve E' defined over $K(j(E))$ (see [Sil09] Chapter III Proposition 1.4). Proposition 2.3.1 ensures that the endomorphisms of E' are defined over $K(j(E))$. □

2.5 The associated Hecke character

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}$. Let F be a finite extension of K and denote by $\mathcal{O}_F$ its ring of integers. Suppose E is an elliptic curve defined over F with complex multiplication by $\mathcal{O}$. In this section we define a Hecke character on F (i.e. a continuous map from $\mathbb{A}_F^\times \to \mathbb{C}^\times$ which is trivial on $F^\times$) associated to E

$$\psi_E : \mathbb{A}_F^\times \to \mathbb{C}^\times.$$

This character is very useful because it contains the information about how the action of $[x, F]$ with $x \in \mathbb{A}_F^\times$ on the torsion points, E_{tors}, translates to multiplication by some element that will be related to $\psi_E(x)$. Of course, the definition of ψ_E is based on the Main Theorem.

The next proposition allows to define a map from the idele group of F to $K^\times$, that, after a modification, will become the desired Hecke character.

Proposition 2.5.1. *There is a unique morphism*

$$\alpha_{E/F} : \mathbb{A}_F^\times \to K^\times$$

such that if $x \in \mathbb{A}_F^\times$ and $s = \mathrm{N}_{F/K}x \in \mathbb{A}_K^\times$, then $\alpha = \alpha_{E/F}(x)$ is the unique element of $K^\times$ satisfying:

1. $\alpha\mathcal{O} = (s)$,

2. *For any fractional ideal* $\mathfrak{a}$ *and analytic isomorphism such that*

$$f : \mathbb{C}/\mathfrak{a} \xrightarrow{\sim} E(\mathbb{C})$$

we have the commutative diagram

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{f} & E(F^{\mathrm{ab}}) \\ \downarrow{\scriptstyle \alpha s^{-1}} & & \downarrow{\scriptstyle [x,F]} \\ K/\mathfrak{a} & \xrightarrow{f} & E(F^{\mathrm{ab}}). \end{array}$$

Remark 2.5.2. Since $K \subset F$, Proposition 2.3.2 tells us that the $F(E[\mathfrak{a}])$ is an abelian extension of F. Hence, $F(E_{\mathrm{tors}}) \subset F^{\mathrm{ab}}$. This shows that $f(K/\mathfrak{a}) \subset E(F^{\mathrm{ab}})$ as we can see in the previous diagram.

Proof. Extend $[x, F]$ to an element $\sigma \in \mathrm{Aut}(\mathbb{C}/F)$ and let $s = N_{F/K}(x) \in \mathbb{A}_K^\times$. Notice that $[s, K] = \sigma|_{K^{\mathrm{ab}}}$. Take a fractional ideal $\mathfrak{a}$ such that $\mathbb{C}/\mathfrak{a}$ is isomorphic to $E(\mathbb{C})$ via an analytic isomorphism f. We can apply the Main Theorem (Theorem 2.4.4) with f, σ and s to obtain a commutative diagram

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{f} & E(\mathbb{C}) \\ \downarrow{\scriptstyle s^{-1}} & & \downarrow{\scriptstyle \sigma} \\ K/s^{-1}\mathfrak{a} & \xrightarrow{f'} & E^\sigma(\mathbb{C}). \end{array}$$

Where $f' : \mathbb{C}/s^{-1}\mathfrak{a} \to E^\sigma(\mathbb{C})$ is an analytical isomorphism. But since E is defined over F and σ fixes F we have $E = E^\sigma$. Hence

$$\mathbb{C}/s^{-1}\mathfrak{a} \xrightarrow{f'} E(\mathbb{C}) \xrightarrow{f^{-1}} \mathbb{C}/\mathfrak{a}$$

is an isomorphism. Therefore there exists $\alpha \in \mathbb{C}^\times$ such that $(\cdot\alpha) = f^{-1} \circ f$ and

$$\alpha s^{-1}\mathfrak{a} = \mathfrak{a} \implies \alpha\mathcal{O}_K = (s).$$

This proves the first assertion of the proposition (and it also implies $\alpha \in K^\times$) and, noting that $\cdot\alpha \circ s^{-1} = \alpha s^{-1}$ it allows us to write

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{f} & E(\mathbb{C}) \\ \downarrow{\scriptstyle \alpha s^{-1}} & & \downarrow{\scriptstyle \sigma} \\ K/\mathfrak{a} & \xrightarrow{f} & E(\mathbb{C}). \end{array}$$

Finally, the image of $K/\mathfrak{a}$ by f lies in $E_{\text{tors}} \subset F^{\text{ab}}$ and $\sigma|_{F^{\text{ab}}} = [x, F]$ we can substitute $E(\mathbb{C})$ for $E(F^{\text{ab}})$ and σ for $[x, F]$ obtaining the desired commutative diagram.

To see that α is unique suppose that there exists $\alpha' \in K^\times$ making the diagram commutative. This means that $(\alpha s^{-1}) = (\alpha' s^{-1})$ and since $(\alpha' s^{-1})$ is invertible with inverse $(s\alpha'^{-1})$ we have

$$t = (\alpha s^{-1}) \circ (s\alpha'^{-1})t = \alpha \cdot \alpha'^{-1} t \quad \text{for all } t \in K/\mathfrak{a}.$$

This yields

$$(1 - \alpha\alpha'^{-1})K \subset \mathfrak{a}$$

the only possibility is $\alpha\alpha'^{-1} = 1$. Note that the fact that α is a morphism follows from the unicity of α because $\alpha(x)\alpha(y)$ satisfies the condition that $\alpha(xy)$ should satisfy.

Finally, we need to see that α does not depend on the choice of $\mathfrak{a}$ and f. Let $\mathfrak{a}'$ be fractional ideal such that $f' : \mathbb{C}/\mathfrak{a}' \xrightarrow{\sim} E(\mathbb{C})$. Note that $f^{-1} \circ f' : \mathbb{C}/\mathfrak{a}' \to \mathbb{C}/\mathfrak{a}$ is an analytic automorphism. Therefore, there exists $\gamma \in \mathbb{C}$ such that the map $f^{-1} \circ f'$ corresponds to multiplication by γ. This is, $\mathfrak{a}'\gamma = \mathfrak{a}$ and $f'(z) = f(\gamma z)$. Thus, for any $z \in K/\mathfrak{a}'$ and $[x, F]$, if we use that the diagram commutes for f and $\mathfrak{a}$

$$f'(x)^{[x,F]} = f(\gamma z)^{[x,F]} = f\left(\alpha s^{-1})\gamma z\right) = f'\left((\alpha s^{-1})z\right).$$

□

Theorem 2.5.3. *Recall the map $\alpha_{E/F}$ from Proposition 2.5.1. Then the following map $\psi_{E/F} = \psi$ is a Hecke character*

$$\psi : \mathbb{A}_F^\times \to \mathbb{C}^\times, \quad \psi(x) = \alpha_{E/F}(x)\mathrm{N}_{F/K}(x^{-1})_\infty.$$

Here $\mathrm{N}_{F/K}(x^{-1})_\infty \in \mathbb{C}^\times$ stands for the unique infinite component of $\mathrm{N}_{F/K}(x^{-1}) \in \mathbb{A}_K^\times$ (K is an imaginary quadratic field).

Proof. Fix $\mathfrak{a}$ an ideal of K such that $f : \mathbb{C}/\mathfrak{a} \to E(\mathbb{C})$ is an isomorphism. We need to prove that ψ is a morphism, $\psi(F^\times) = 1$ and that ψ is continuous. We will do it in this order:

1. ψ is a morphism: the norm map is a morphism from the group $\mathbb{A}_F^\times$ to $\mathbb{A}_K^\times$, so its restriction to the ∞ component is still a morphism. The inversion $x \mapsto x^{-1}$ is also a morphism ($\mathbb{A}_F^\times$ is a topological group), thus, we obtain a morphism if we compose this maps: $\mathrm{N}_{F/K}(x^{-1})_\infty$. We already saw that $\alpha_{E/F}$ is a morphism so we are done.

2. $\psi(F^\times) = 1$: let $\beta \in F$ and $x = (\beta, \beta, \dots) \in \mathbb{A}_F^\times$. We have to see that $\alpha(x) = \mathrm{N}_{F/K}(x)_\infty$. Since x is a principal idele, $[x, F] = \mathrm{id}$, and by Proposition 2.5.1

$\alpha \in K^\times$ is the unique element such that multiplication by $\alpha \mathrm{N}_{F/K}(x)^{-1}$ is the identity on $K/\mathfrak{a}$. This is equivalent to $\alpha \cdot \left(\mathrm{N}_{F/K}(x)^{-1}\right)_{\mathfrak{p}}$ is the identity in $K_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}}$ for every $\mathfrak{p}$ of K. Using that for all primes (finite and infinite) v of K

$$\mathrm{N}_{F/K}(\beta) = \prod_{w|v} \mathrm{N}_{F_w/K_v}(\beta) = \left(\mathrm{N}_{F/K}(x)\right)_v \tag{2.1}$$

we see that $\alpha = \mathrm{N}_{F/K}(\beta)$. Applying (2.1) for $v = \infty$ we get that $\psi(\beta) = 1$.

3. ψ is continuous: $\mathbb{A}_F^\times$ is a topological group, so it is enough to find a nonempty open set U where ψ is continuous. Note that inversion, the norm map $\mathrm{N}_{F/K}$ and its restriction to the ∞ component are continuous, hence $\mathrm{N}_{F/K}(x^{-1})_\infty$ is continuous. Therefore it is enough to find a nonempty open $U \subset \mathbb{A}_F^\times$ such that $\psi(x) = \mathrm{N}_{F/K}(x^{-1})_\infty$ if $x \in U$.

   Let $m \geq 3$ and B_m the preimage of $\mathrm{Gal}(F^{\mathrm{ab}}/F(E[m]))$ by the Artin map. Hence B_m is an open set. Let

$$W_m = \left\{ s \in \mathbb{A}_K^\times \mid s_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^\times, s_{\mathfrak{p}} \in 1 + m\mathcal{O}_{\mathfrak{p}} \text{ for all } \mathfrak{p} \right\},$$

   and

$$U = B_m \cap \left\{ x \in \mathbb{A}_F^\times \mid \mathrm{N}_{F/K}(x) \in W_m \right\}.$$

   which is open and nonempty. If $x \in U$ then $s = \mathrm{N}_{F/K}(x) \in W_m$ and $[x, F]|_{E[m]} = \mathrm{id}$. Applying Proposition 2.5.1 to determine $\alpha(x) = \alpha$ we obtain the commutative diagram

$$\begin{array}{ccc} m^{-1}\mathfrak{a}/\mathfrak{a} & \xrightarrow{f} & E[m] \\ \downarrow{\scriptstyle \alpha s^{-1}} & & \downarrow{\scriptstyle \mathrm{id}} \\ m^{-1}\mathfrak{a}/\mathfrak{a} & \xrightarrow{f} & E[m]. \end{array}$$

   Since $s \in W_m$ the map s^{-1} is the identity in $m^{-1}\mathfrak{a}/\mathfrak{a}$. Thus, for every $t \in m^{-1}\mathfrak{a}/\mathfrak{a}$

$$f(t) = f(\alpha t) \implies t - \alpha t \in \mathfrak{a} \text{ for all } t \in m^{-1}\mathfrak{a} \implies m^{-1}\mathfrak{a}(1-\alpha) \subset \mathfrak{a}.$$

   This implies $\alpha \equiv 1 \mod m\mathcal{O}$. But Proposition 2.5.1 also tells us that $\alpha\mathcal{O} = (s) = \mathcal{O}$ where the last equality follows from $s \in W_m$, therefore $\alpha \in \mathcal{O}^\times$. So we get that $\alpha \in \mathcal{O}^\times$ such that $m \mid (\alpha - 1)$, in particular $\mathrm{N}_{K/\mathbb{Q}}(m) \mid \mathrm{N}_{K/\mathbb{Q}}(\alpha - 1)$. Now, Dirichlet's unit theorem applied to an imaginary quadratic field K tells us that the only units are roots of unity. More precisely the units can only be the roots of unity in μ_2, μ_4 or μ_6. For all of them $9 > N_{K/\mathbb{Q}}(\alpha - 1)$ so the only possibility is $\alpha = 1$ and the result follows.

□

Definition 2.5.4. The Hecke character associated to E, denoted by $\psi_{E/F}$ or just ψ, is the Hecke character of Theorem 2.5.3. We will denote by $\alpha_{E/F}(x)$ or just $\alpha(x)$ or α (if x is clear) its finite part.

The next lemma is useful since it will tell us when the map multiplication by $x \in \mathbb{A}_K^\times$ is the identity. Using the Hecke character this translates to characterize when some automorphisms act trivially in certain torsion subgroups.

Lemma 2.5.5. *Let $\mathfrak{b}$ be an integral ideal of $\mathcal{O}$ and $\mathfrak{a}$ a fractional ideal of K. Consider an idele $x \in \mathbb{A}_K^\times$ such that $\mathrm{ord}_\mathfrak{p}(x_\mathfrak{p}) = 0$ for all $\mathfrak{p}$ finite prime of K. The map*

$$\mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a} \xrightarrow{\cdot x} \mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a}$$

is the identity if and only if $x_\mathfrak{p} \equiv 1 \mod \mathfrak{b}_\mathfrak{p}$ for all primes dividing $\mathfrak{b}$.

Proof. First note that this map is the restriction of the map in Definition 2.4.2 on $\mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a}$ and it is well defined because we imposed that $\mathrm{ord}_\mathfrak{p}(x_\mathfrak{p}) = 0$ at every prime $\mathfrak{p}$.

We use the decomposition

$$\begin{array}{ccc} \mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a} & \xrightarrow{\cdot x} & \mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a} \\ \downarrow\wr & & \downarrow\wr \\ \bigoplus_\mathfrak{p} \mathfrak{b}_\mathfrak{p}^{-1}\mathfrak{a}_\mathfrak{p}/\mathfrak{a}_\mathfrak{p} & \xrightarrow{(\cdot x_\mathfrak{p})} & \bigoplus_\mathfrak{p} \mathfrak{b}_\mathfrak{p}^{-1}\mathfrak{a}_\mathfrak{p}/\mathfrak{a}_\mathfrak{p} \end{array}$$

to affirm that $\cdot x$ is the identity if and only $\cdot x_\mathfrak{p}$ is the identity for every prime $\mathfrak{p}$ dividing $\mathfrak{b}$. Now, $x_\mathfrak{p}$ is the identity if and only if, for every $t_\mathfrak{p} \in \mathfrak{b}_\mathfrak{p}^{-1}\mathfrak{a}_\mathfrak{p}$

$$t_\mathfrak{p} x_\mathfrak{p} - t_\mathfrak{p} \in \mathfrak{a}_\mathfrak{p} \iff t_\mathfrak{p}(x_\mathfrak{p} - 1) \in \mathfrak{a}_\mathfrak{p} \iff \mathfrak{b}_\mathfrak{p}^{-1}\mathfrak{a}_\mathfrak{p}(x_\mathfrak{p} - 1) \in \mathfrak{a}_\mathfrak{p} \iff x_\mathfrak{p} - 1 \in \mathfrak{b}_\mathfrak{p}.$$

□

Our goal for the rest of this section is to, given the Hecke character ψ, define its corresponding character in terms of ideals. We will also relate the conductor of this character with the primes where E has bad reduction.

Definition 2.5.6. The conductor of ψ is the largest ideal $\mathfrak{F}$ of $\mathcal{O}_F$ such that $\psi(x) = 1$ for all finite ideles $x = (x_\mathfrak{P}) \in \mathbb{A}_F^\times$ such that $x_\mathfrak{P} \in \mathcal{O}_{F,\mathfrak{P}}^\times$ for all $\mathfrak{P}$ and $x_\mathfrak{P} \in 1 + \mathfrak{F}\mathcal{O}_{F,\mathfrak{P}}$ for all $\mathfrak{P} \mid \mathfrak{F}$.

Definition 2.5.7. The Hecke character attached to E in terms of ideals, also denoted by ψ, is defined as follows: if $\mathfrak{P}$ is a prime ideal of F coprime to $\mathfrak{F}$ define $\psi(\mathfrak{P}) = \psi(x)$ where $x = (1, \dots, 1, \pi, 1, \dots)$ and $\pi \in \mathcal{O}_{F,\mathfrak{P}}$ is a uniformizer. Extend the definition to $\psi(\mathfrak{B})$ for all ideals $\mathfrak{B}$ of F coprime to $\mathfrak{F}$ multiplicatively.

Remark 2.5.8. The existence of a conductor follows from the continuity of ψ and the topology of $\mathbb{A}_F^\times$. It can be found in Chapter 6 of [Neu13, p. 480,481] pages 480 and 481.

Proposition 2.5.9. *Let $\mathfrak{P}$ be a prime of F. Then $\psi(\mathcal{O}_{F,\mathfrak{P}}^\times) = 1$ if and only if E has good reduction at $\mathfrak{P}$.*

Proof. We will use Theorem 1.4.8: E/F has good reduction at the prime $\mathfrak{P}$ if and only if the inertia subgroup $I_\mathfrak{P}$ acts trivially on $E[m]$ for infinitely many integers m prime to $\mathfrak{P}$. Since the torsion points lie on abelian extensions of F, it is enough to work with the quotient of the inertia subgroup, $I_\mathfrak{P}^{\mathrm{ab}} \subset \mathrm{Gal}(F^{\mathrm{ab}}/F)$. Recall that, by class field theory $[\mathcal{O}_{F,\mathfrak{P}}^\times, F] = I_\mathfrak{P}^{\mathrm{ab}}$.

Let $x \in \mathcal{O}_{F,\mathfrak{P}}^\times$ and also denote by $x \in \mathbb{A}_F^\times$ the idele with ones in all the components except in the $\mathfrak{P}$-component where it equals to x. Let $m \in \mathbb{Z}$ coprime to $\mathfrak{P}$. We can take a fractional ideal $\mathfrak{a}$ and an isomorphism f such that $f : \mathbb{C}/\mathfrak{a} \xrightarrow{\sim} E$. The action of $[x, L]$ on $E[m]$ is described as

$$\begin{array}{ccc} (m)^{-1}\mathfrak{a}/\mathfrak{a} & \xrightarrow{f} & E[m] \\ \downarrow{\scriptstyle \alpha(x)s^{-1}} & & \downarrow{\scriptstyle [x,F]} \\ (m)^{-1}\mathfrak{a}/\mathfrak{a} & \xrightarrow{f} & E[m] \end{array}$$

where (m) is the ideal generated by m in $\mathcal{O}$ and $s = \mathrm{N}_{F/K}(x) \in \mathbb{A}_K^\times$. Looking at the expression of x we deduce from Lemma 2.5.5 that multiplication by s^{-1} acts as the identity since $\mathfrak{P}$ does not divide m. Using the lemma again

$$[x, F]|_{E[m]} = 1 \iff \alpha(x) \equiv 1 \mod (m).$$

From here

$$[x, F]|_{E[m]} = 1 \text{ for infinitely many } m \text{ coprime to } \mathfrak{P} \iff \alpha(x) = 1.$$

And now the result follows because x is a finite idele so $\alpha(x) = \psi(x)$. □

Corollary 2.5.10. *If a prime ideal $\mathfrak{P}$ of F does not divide $\mathfrak{F}$, then E has good reduction at the prime $\mathfrak{P}$.*

Proof. Let $x = (x_\mathfrak{Q}) \in \mathbb{A}_F^\times$ be a finite idele such that $x_\mathfrak{P} = u \in \mathcal{O}_{F,\mathfrak{P}}^\times$ and $x_\mathfrak{Q} = 1$ for all $\mathfrak{Q} \neq \mathfrak{P}$. Then, for any prime $\mathfrak{Q}$ dividing $\mathfrak{F}$, $x_\mathfrak{Q} = 1 \in 1 + \mathfrak{F}\mathcal{O}_{F,\mathfrak{P}}$, so $\psi(x) = 1$. Therefore $\psi(\mathcal{O}_{F,\mathfrak{P}}^\times) = 1$ and Proposition 2.5.9 implies the result. □

Proposition 2.5.11. *For $\mathfrak{P}$ a prime ideal of F coprime to $\mathfrak{F}$ let*

$$[\psi(\tilde{\mathfrak{P}})] : \tilde{E} \to \tilde{E}$$

be the reduction of $\psi(\mathfrak{P}) : E \to E$ introduced in Definition 1.3.8. Then $[\psi(\tilde{\mathfrak{P}})]$ coincides with

$$\varphi_q : \tilde{E} \to \tilde{E}, \quad (x, y) \mapsto (x^q, y^q),$$

where $q = \mathrm{N}_{F/\mathbb{Q}}$, the so called q-Frobenius endomorphism.

Proof. Choose $x \in \mathbb{A}_F^\times$ finite such that $x = (1, \dots, 1, \pi, 1, \dots)$ where $\pi \in \mathcal{O}_{F,\mathfrak{P}}$ is a uniformizer. Since x is a finite idele we see that $\alpha = \alpha(x) = \psi(\mathfrak{P})$. By Proposition 2.5.1, $\alpha\mathcal{O} = N_{F/K}\mathfrak{P}$, in particular $\alpha \in \mathcal{O}$. To see that α reduces to φ_q we will see that the kernel of $\widetilde{[\alpha]} - \varphi_q$ is arbitrarily large, which implies that $\widetilde{[\alpha]} - \varphi_q = 0$ since 0 is the only isogeny with infinite kernel.

Let $m \in \mathbb{Z}$ be an integer coprime to $\mathfrak{P}$ and $P \in E[m]$. The main theorem of complex multiplication translates the action of $[x, F]$ on $E[m]$ to multiplication by $\alpha \mathrm{N}_{F/K} x^{-1}$. But m is coprime to $\mathfrak{P}$ so Lemma 2.5.5 shows that $\mathrm{N}_{F/K} x^{-1}$ acts trivially on $E[m]$. Therefore

$$[\alpha]P = P^{[x,F]}.$$

By class field theory, since $x = (1, \dots, 1, \pi, 1, \dots)$, $[x, F]$ restricts to the $\mathfrak{P}$-Frobenius automorphism of the unramified extension $F(E[m])/F$ which implies

$$\widetilde{[\alpha]}\tilde{P} = \widetilde{[\alpha]P} = \widetilde{P^{[x,F]}} = \varphi_q(\tilde{P})$$

where the reduction is modulo some prime above $\mathfrak{P}$. Now, since E has good reduction at $\mathfrak{P}$ it also has good reduction at a prime above $\mathfrak{P}$ in the extension $K(E[m])$ so we can apply Proposition 1.4.4 to see that $E[m]$ injects on $\tilde{E}$. Hence

$$E[m] \subset \ker(\widetilde{[\alpha]} - \varphi_q).$$

Since m can be arbitrarily large the result follows

□

2.6 Consequences of the Main Theorem

In this chapter we present some consequences of the Main Theorem that will be very useful in for the proof of Coates–Wiles Theorem.

Corollary 2.6.1. *Suppose E is defined over K (i.e. $F = K$). Denote by $\mathfrak{f}$ the conductor of ψ. Then:*

1. *The reduction map* $\mathcal{O}^\times \to (\mathcal{O}/\mathfrak{f})^\times$ *is injective.*

2. *The elliptic curve* E *does not have good reduction at all primes of* K*.*

Proof. 1. Let $u \in \mathcal{O}^\times$ be distinct from 1. Consider the idele $x \in \mathbb{A}_K^\times$ such that $x_\infty = 1$ and $x_\mathfrak{p} = u$ for all finite primes $\mathfrak{p}$. Also denote by u the constant idele of $\mathbb{A}_K^\times$ that has u in all coordinates and note $\psi(u) = 1$. We proceed to compute $\psi(x)$

$$\psi(x) = \psi(u)^{-1}\psi(x) = \psi(u^{-1}x) = \alpha(u^{-1}x)u^{-1}.$$

Where in the last equallity we used the definition of the Hecke character in Theorem 2.5.3 and the fact that the infinte part of $u^{-1}x$ is u^{-1}.

In order to compute $\alpha(u^{-1}x)$ we see that $u^{-1}x = (u^{-1}, 1, 1, \dots)$ so by class field theory $[u^{-1}x, K] = 1$ (because the completion of K with respect to the infinite prime is $\mathbb{C}$). Hence, by the uniqueness part of Proposition 2.5.1 we get that $\alpha(u^{-1}x) = 1$. Thus, $\psi(x) = u^{-1} \neq 1$ so we just have to use the definition of the conductor to conclude that $u \not\equiv 1 \mod \mathfrak{f}$.

2. For the sake of contradiction suppose that E has good reduction at all primes $\mathfrak{p}$ of K. Then consider the following sequence of ideles $(a_i)_{i\in\mathbb{N}} \subset \mathbb{A}_K^\times$.

$$a_1 = (1, u, 1, 1, \dots), a_2 = (1, u, u, 1, 1, \dots), a_3 = (1, u, u, u, 1, 1, \dots), \dots$$

so there are only a finitely many terms distinct to 1. Using that we have good reduction at all primes, by Proposition 2.5.9 we can deduce the $\psi(a_i) = 1$ for all i. This sequence converges to x (where $\mathbb{A}_K^\times$ has the usual topology) and by the continuity of ψ we should have $\psi(x) = 1$. This is a contradiction since we already had $\psi(x) = u^{-1} \neq 1$.

□

Corollary 2.6.2. *Suppose* E *is defined over* K*. Let* $\mathfrak{p}$ *be a prime ideal of* K*. Suppose that the reduction map* $\mathcal{O}^\times \to \left(\mathcal{O}/\mathfrak{p}\right)^\times$ *is not surjective. Then* $E[\mathfrak{p}] \not\subset E(K)$*.*

Proof. We are going to prove the contrapositive statement, so suppose that $E[\mathfrak{p}] \subset E(K)$. Let $z \in (\mathcal{O}/\mathfrak{p})^\times$, we are going to find $\alpha \in \mathcal{O}$ that maps to z.

We can take $u \in \mathcal{O}_\mathfrak{p}^\times$ such that u reduces to z modulo the prime ideal of $\mathcal{O}_\mathfrak{p}$ and let $x = (1, \dots, 1, u, 1, \dots) \in \mathbb{A}_K^\times$ where $x_\mathfrak{p} = u$. By hypothesis, $[x, K]$ is the identity when restricted to the elements of $E[\mathfrak{p}]$. Using Proposition 2.5.1 (2) and (1), this action translates to multiplication by $\alpha(x)x^{-1}$, where $\alpha(x) \in \mathcal{O}^\times$ and since $\alpha(x)x^{-1}$ is the identity on the $\mathfrak{p}$ torsion points Lemma 2.5.5 implies that $(\alpha(x)x^{-1})_\mathfrak{p} \equiv 1 \mod \mathfrak{p}$. Hence

$$\alpha(x) = \alpha(x)_\mathfrak{p} \equiv u \equiv z \mod \mathfrak{p}.$$

So the reduction map is surjective. □

Remark 2.6.3. In this proof we denoted as $\mathfrak{p}$ the prime ideal of $\mathcal{O}_\mathfrak{p}$ in order to simplify the notation.

Theorem 2.6.4. *Suppose E is defined over K and denote by $\mathfrak{f}$ the conductor of ψ. Let $\mathfrak{b}$ be an integral ideal of $\mathcal{O}$ coprime with $\mathfrak{f}$ and $\mathfrak{p}$ a prime ideal of $\mathcal{O}$ not dividing $\mathfrak{f}$. Then,*

1. *The torsion points $E[\mathfrak{bf}]$ are defined in the ray class field of K modulo $\mathfrak{bf}$, i.e. $E[\mathfrak{bf}] \subset K(\mathfrak{bf})$.*
2. *The map $\mathrm{Gal}(K(E[\mathfrak{b}])/K) \to (\mathcal{O}/\mathfrak{b})^\times$ of Proposition 2.3.2 is an isomorphism.*
3. *If $\mathfrak{c} \mid \mathfrak{b}$ then the natural map $\mathrm{Gal}(K(\mathfrak{bf})/K(\mathfrak{cf})) \to \mathrm{Gal}(K(E[\mathfrak{b}])/K(E[\mathfrak{c}]))$ is an isomorphism.*
4. *The extension $K(E[\mathfrak{p}^n\mathfrak{b}])/K(E[\mathfrak{b}])$ is totally ramified at all primes above $\mathfrak{p}$.*
5. *If the map $\mathcal{O}^\times \to (\mathcal{O}/\mathfrak{b})^\times$ is injective then $K(E[\mathfrak{p}^n\mathfrak{b}])/K(E[\mathfrak{b}])$ is unramified outside $\mathfrak{p}$.*

Proof. For an integral ideal $\mathfrak{c}$, denote by $U_\mathfrak{c} = \left\{ s \in \mathbb{A}_K^\times \mid s_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times \text{ and } s_\mathfrak{p} \in 1 + \mathfrak{c}\mathcal{O}_\mathfrak{p} \text{ for all } \mathfrak{p} \right\}$. Class field theory tells us that

$$[\,.\,, K] : \mathbb{A}_K^\times / \left(K^\times U_\mathfrak{c} \right) \xrightarrow{\sim} \mathrm{Gal}(K(\mathfrak{c})/K).$$

Consider also the prime factorizations of $\mathfrak{b} = \prod_{i=1}^k \mathfrak{q}_i^{e_i(\mathfrak{b})}$ and $\mathfrak{c} = \prod_{i=1}^k \mathfrak{q}_i^{e_i(\mathfrak{c})}$. Finally, fix a fractional ideal $\mathfrak{a}$ and analytic isomorphism $f : \mathbb{C}/\mathfrak{a} \xrightarrow{\sim} E$.

1. By the previous statement of class field theory it is enough to see that for every $x \in K^\times U_\mathfrak{bf}$, $[x, K]$ acts trivially on $E[\mathfrak{bf}]$: first note that we can suppose that x is finite, because K imaginary quadratic implies that the infinite component does not affect on $[x, K]$. We can also suppose that $x \in U_\mathfrak{bf}$ since $[k, K] = 1$ if $k \in K^\times$.

   Now, the action of $[x, K]$ on $E[\mathfrak{bf}]$ translates to multiplication by $\alpha(x)x^{-1}$ in $(\mathfrak{bf})^{-1}\mathfrak{a}/\mathfrak{a}$. Since $x_\mathfrak{q} \in 1 + \mathfrak{f}\mathcal{O}_\mathfrak{q}$ for all $\mathfrak{q}$ and x is finite $\alpha(x) = \psi(x) = 1$, and since $x_\mathfrak{q} \in 1 + \mathfrak{b}\mathcal{O}_\mathfrak{q}$ for all $\mathfrak{q}$ Lemma 2.5.5 ensures that multiplication by x^{-1} is the identity and we are done.

2. We already know that the map of the statement is an injective morphism. In order to prove that the map is a bijection we will find $\#(\mathcal{O}/\mathfrak{b})^\times$ distinct elements of $\mathrm{Gal}(K(E[\mathfrak{b}])/K)$.

   For every element of $x \in \mathcal{O}_{\mathfrak{q}_i}^\times \subset \mathbb{A}_K^\times$, $[x, K]$ acts on $E[\mathfrak{b}]$ as multiplication by x^{-1} on $\mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a}$ ($\mathfrak{b}$ is coprime to $\mathfrak{f}$ so we have $\alpha(x) = 1$). Using the prime factorization

of $\mathfrak{b}$, Lemma 2.5.5 tells us that $(\cdot x^{-1})$ is the identity exaclty when $x \in 1+\mathfrak{q}^{e_i(\mathfrak{b})}\mathcal{O}_{\mathfrak{q}_i}$. Hence, for every i we have

$$\mathcal{O}_{\mathfrak{q}_i}^{\times}/\left(1+\mathfrak{q}_i^{e_i(\mathfrak{b})}\mathcal{O}_{\mathfrak{q}_i}\right) \hookrightarrow \mathrm{Gal}(K(E[\mathfrak{b}])/K), \quad x \mapsto [x,K]|_{K(E[\mathfrak{b}])}.$$

It is easy to see that we can use these maps to define an injective map

$$\prod_{i=1}^{k} \mathcal{O}_{\mathfrak{q}_i}^{\times}/\left(1+\mathfrak{q}_i^{e_i(\mathfrak{b})}\mathcal{O}_{\mathfrak{q}_i}\right) \hookrightarrow \mathrm{Gal}(K(E[\mathfrak{b}])/K)$$

And now we use the well known isomorphisms of the nth higher unit groups ([**?**] Chapter 2, Prop. 3.10 and Prop. 4.3)

$$\mathcal{O}_{\mathfrak{q}_i}^{\times}/\left(1+\mathfrak{q}_i^{e_i(\mathfrak{b})}\mathcal{O}_{\mathfrak{q}_i}\right) \cong \left(\mathcal{O}_{\mathfrak{q}_i}/{\mathfrak{q}_i}^{e_i(\mathfrak{b})}\mathcal{O}_{\mathfrak{q}_i}\right)^{\times} \cong (\mathcal{O}/\mathfrak{q}_i^{e_i(\mathfrak{b})})^{\times}.$$

From here

$$\#\prod_{i=1}^{k} \mathcal{O}_{\mathfrak{q}_i}^{\times}/\left(1+\mathfrak{q}_i^{e_i(\mathfrak{b})}\mathcal{O}_{\mathfrak{q}_i}\right) = \#\prod_{i=1}^{k}(\mathcal{O}/\mathfrak{q}_i^{e_i(\mathfrak{b})})^{\times} = \#\left(\mathcal{O}/\mathfrak{b}\right)^{\times}.$$

Where we used the Chinese Remainder Theorem for the last equality.

3. From (1), $K(E[\mathfrak{b}]) \subset K(\mathfrak{bf})$ for any ideal $\mathfrak{b}$ coprime to $\mathfrak{f}$ so the map is well defined.

   Let $\sigma \in \mathrm{Gal}(K(\mathfrak{bf})/K(\mathfrak{cf}))$. By class field theory we can choose $x \in \mathbb{A}_K^{\times}$ finite such that $\sigma = [x,K]|_{K(\mathfrak{bf})}$. Moreover, since σ fixes $K(\mathfrak{cf})$ we can take $x \in U_{\mathfrak{cf}}$. Let's see that the map is injective: suppose that σ acts trivially on $E[\mathfrak{b}]$, then translating the action of σ as multiplication by $\alpha(x)x^{-1}$ on $\mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a}$ and noting that $\alpha(x) = \psi(x) = 1$ we see that $x_{\mathfrak{q}} \in 1+\mathfrak{b}\mathcal{O}_{\mathfrak{q}}$ for all primes $\mathfrak{q}$. Since $\mathfrak{b}$ and $\mathfrak{f}$ are coprime $x_{\mathfrak{q}} \in 1+\mathfrak{bf}\mathcal{O}_{\mathfrak{q}}$ for all $\mathfrak{q}$, i.e. $x \in U_{\mathfrak{bf}}$ so $[x,K]$ (and therefore σ) fixes the ray class field $K(\mathfrak{bf})$.

   To prove that it is a bijection we can compare the cardinality of the two groups. From part (2)

$$\#\mathrm{Gal}(K(E[\mathfrak{b}])/K(E[\mathfrak{c}])) = \frac{\#\left(\mathcal{O}/\mathfrak{b}\right)^{\times}}{\#\left(\mathcal{O}/\mathfrak{c}\right)^{\times}} = \prod_{i=1}^{k} \frac{\#\left(\mathcal{O}/\mathfrak{q}_i^{e_i(\mathfrak{b})}\right)^{\times}}{\#\left(\mathcal{O}/\mathfrak{q}_i^{e_i(\mathfrak{c})}\right)^{\times}}. \tag{2.2}$$

   On the other hand, the exact sequence

$$1 \to \mathrm{Gal}(K(\mathfrak{bf})/K(\mathfrak{cf})) \to \mathrm{Gal}(K(\mathfrak{bf})/K) \to \mathrm{Gal}(K(\mathfrak{cf})/K) \to 1$$

and the isomorphism of class field theory stated at the begining of this proof lead to

$$\mathrm{Gal}(K(\mathfrak{b}\mathfrak{f})/K(\mathfrak{c}\mathfrak{f})) \cong \frac{K^\times U_{\mathfrak{c}\mathfrak{f}}}{K^\times U_{\mathfrak{b}\mathfrak{f}}} \cong \frac{K^\times U_{\mathfrak{c}}}{K^\times U_{\mathfrak{b}}},$$

where we used that $\mathfrak{f}$ and $\mathfrak{b}$ are coprime. If we denote $U_{\mathfrak{q}}^{(m)} = (1+\mathfrak{q}^m\mathcal{O}_{\mathfrak{q}})$ if $m > 0$ and $U_{\mathfrak{q}_i}^{(0)} = (\mathcal{O}_{\mathfrak{q}})^\times$ we have, by inspection

$$\frac{K^\times U_{\mathfrak{c}}}{K^\times U_{\mathfrak{b}}} \cong \prod_{i=1}^{k} \frac{U_{\mathfrak{q}_i}^{(e_i(\mathfrak{c}))}}{U_{\mathfrak{q}_i}^{(e_i(\mathfrak{b}))}}$$

Now, as we did in the proof of (2) it is possible to count the number of elements of this group and see that it is equal to the expression of (2.2).

4. Given $x \in U_{\mathfrak{p}}^{(e_{\mathfrak{p}}(\mathfrak{b}))}$, we can translate the action of $[x, K]$ on $E[\mathfrak{p}^n\mathfrak{b}]$ as multiplication by x^{-1} on $\mathfrak{p}^{-n}\mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a}$. Applying Lemma 2.5.5 we see that $[x, K]$ fixes $E[\mathfrak{b}]$ and it is possible to determine for which x the action is trivial. Hence, we have the injection

$$\frac{U_{\mathfrak{p}}^{(e_{\mathfrak{p}}(\mathfrak{b}))}}{U_{\mathfrak{p}}^{(e_{\mathfrak{p}}(\mathfrak{b})+n)}} \hookrightarrow \mathrm{Gal}(K(E[\mathfrak{p}^n\mathfrak{b}])/K(E[\mathfrak{b}])).$$

In fact, this is an isomorphism. This can be seen by comparing the cardinalities of both groups as we did in the previous points. Since $[\mathcal{O}_{\mathfrak{p}}^\times, K] = I_{\mathfrak{p}}^{\mathrm{ab}}$, the inertia group at $\mathfrak{p}$, and $U_{\mathfrak{p}}^{(e_{\mathfrak{p}}(\mathfrak{b}))} \subset \mathcal{O}_{\mathfrak{p}}^\times$ we deduce that the extension is totally ramified at primes above $\mathfrak{p}$.

5. Let $\mathfrak{q}$ be a prime of K, $\mathfrak{p} \neq \mathfrak{q}$. Suppose that $\sigma \in I_{\mathfrak{q}}^{\mathrm{ab}}$ such that σ fixes $E[\mathfrak{b}]$. We are going to prove that then σ fixes $E[\mathfrak{p}^n\mathfrak{b}]$ so therefore the inertia group at primes above $\mathfrak{q}$ is trivial, i.e. the extension is unramified at primes above $\mathfrak{q}$.

   Let $x \in \mathcal{O}_{\mathfrak{q}}^\times$ satisfying that $[x, K] = \sigma$. Then the action of $[x, K]$ on E_{tors} translates to multiplication by $\alpha(x)x^{-1}$ on $K\mathfrak{a}/\mathfrak{a}$, with $\alpha(x) \in \mathcal{O}^\times$. Consider the following two cases:

   - If $\mathfrak{q} \nmid \mathfrak{f}$, then $\alpha(x) = 1$, so the condition that $[x, K]$ fixes $E[\mathfrak{b}]$ implies that $x_{\mathfrak{s}} \in 1 + \mathfrak{b}\mathcal{O}_{\mathfrak{s}}$ for all primes $\mathfrak{s}$ of K. But $x \in \mathcal{O}_{\mathfrak{q}}^\times \subset \mathbb{A}_K^\times$ so $x_{\mathfrak{p}} = 1$ and therefore we will also have $x_s \in 1 + \mathfrak{p}^n\mathfrak{b}\mathcal{O}_{\mathfrak{s}}$ for all primes $\mathfrak{s}$. Thus $[x, K]$ fixes $E[\mathfrak{p}^n\mathfrak{b}]$.
   - If $\mathfrak{q} \mid \mathfrak{f}$, from the condition $\alpha(x)x_{\mathfrak{s}}^{-1} \in 1 + \mathfrak{b}\mathcal{O}_{\mathfrak{s}}$ and the fact that $\mathfrak{f}$ coprime with $\mathfrak{b}$ we deduce that $\alpha \equiv 1 \mod \mathfrak{b}$. But by hypothesis, the reduction map is injective. Thus, $\alpha(x) = 1$. From here it is easy to deduce that $[x, K]$ fixes $E[\mathfrak{p}^n\mathfrak{b}]$.

□

Proposition 2.6.5. *Suppose $\mathfrak{Q}$ is a prime of F. Then there is an elliptic curve E' defined over F satisfying the following two conditions:*

- *The curves E and E' are isomorphic over $\bar{F}$,*
- *the curve E' has good reduction at $\mathfrak{Q}$.*

Proof. Using the characterization of Proposition 2.5.9 we need to find a curve E' such that $\psi_{E'}(\mathcal{O}_{F,\mathfrak{Q}}^{\times}) = 1$. Define the following character

$$\chi : \mathbb{A}_F^{\times}/F^{\times} \to \mathcal{O}_{F,\mathfrak{Q}}^{\times} \xrightarrow{\psi_E} \mathcal{O}^{\times},$$

which is well defined because $\psi_E(\mathcal{O}_{F,\mathfrak{Q}}^{\times}) \subset \mathcal{O}^{\times}$ (Proposition 2.5.1).

By class field theory χ induces a morphism in $\mathrm{Hom}(G_F, \mathcal{O}^{\times})$ which we will also denote by χ. Noting that G_F fixes $\mathcal{O}^{\times}$, if we let $\omega = \#\mathcal{O}^{\times}$, i.e. $\mathcal{O}^{\times} = \mu_{\omega}$, we have:

$$\mathrm{Hom}(G_F, \mathcal{O}^{\times}) = H^1(F, \mu_{\omega}) \cong F^{\times}/F^{\times\omega}.$$

where the last isomorphism is given by the Kummer map and it is ensured by the Hilbert's Theorem 90. Hence, there exists $d \in F^{\times}$ such that, for every $\sigma \in F_K$

$$\chi(\sigma) d^{1/\omega} = \left(d^{1/\omega}\right)^{\sigma}.$$

If $E : y^2 = x^3 + ax + b$, with $a, b \in F$ consider consider the following curve E' (which depends on ω)

$$E' = \begin{cases} y^2 = x^3 + d^2ax + d^3b & \text{if } \omega = 2 \\ y^2 = x^3 + dax & \text{if } \omega = 4 \\ y^2 = x^3 + db & \text{if } \omega = 6 \end{cases}$$

which is isomorphic to E over $F(d^{1/\omega})$ via the isomorphism $\phi : E \to E'$

$$(x, y) \mapsto \begin{cases} (dx, d^{3/2}y) & \text{if } \omega = 2 \\ (d^{1/2}x, d^{3/4}y) & \text{if } \omega = 4 \\ (d^{1/3}x, d^{1/2}y) & \text{if } \omega = 6. \end{cases}$$

For every $\sigma \in G_F$, $\chi(\sigma) \in \mathcal{O}^{\times}$, and hence $[\chi]$ is an automorphism of both E and E'. In fact it is precisely $[\chi(\sigma)](x, y) = (\chi(\sigma)^2 x, \chi(\sigma)^3 y)$ (see [Sil09] Chapter III, Corollary 10.2). From this expression it is easy to check that

$$\sigma(\phi P) = [\chi(\sigma)^{-1}]\sigma P.$$

It is plain to deduce that $\psi_{E'} = \chi^{-1}\psi_E$, i.e. $\psi_{E'}(\mathcal{O}_{F,\mathfrak{Q}}^{\times}) = 1$ which shows that E' has good reduction over $\mathfrak{Q}$.

□

Chapter 3

Selmer group

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}$. The goal of this chapter is to give the expression of the π^n-Selmer group of an elliptic curve E/K with complex multiplication by $\mathcal{O}$ which we will denote as $S_{\pi^n}(E_{/K})$ (where $\pi \in \mathcal{O}$ is prime).

This expression will allow us to characterize when $S_\pi(E_{/K}) = 0$ which is one of the key points to prove the Coates–Wiles Theorem since, as we will recall in the first section, $S_\pi(E_{/K}) = 0$ implies that $E(K)$ is finite.

In the first section we review the definition of the Selmer group and explain why it can give information about the rank of the curve using the Mordell–Weil Theorem. After some lemmas about cohomology, the last two sections are the calculation of an expression of the Selmer Group $S_{\pi^n}(E_{/K})$. As we will explain, the Selmer group is defined by local conditions, so following what is done in [Rub99] Section 6, we will treat separately these local conditions at the prime $\mathfrak{q}$ depending on whether $\mathfrak{q}$ is coprime to π (section 3) or $\mathfrak{q}$ divides π (section 4).

3.1 Definition of the Selmer group

For this section suppose that E is an elliptic curve defined over a number field F. Denote by $G_F = \mathrm{Gal}(\bar{F}/F)$.

Recall the weak Mordell–Weil Theorem, which is needed to prove the Mordell–Weil Theorem.

Theorem 3.1.1 (Weak Mordell–Weil Theorem)**.** *Let m be an integer, then the group $E(F)/mE(F)$ is finite.*

Proof. See Silverman [Sil09] Chapter VII Theorem 1.1. □

The weak Mordell–Weil Theorem can be generalized to any endomorphism α, i.e., $E(F)/\alpha E(F)$ is finite. The size of $E(F)/\alpha E(F)$ can give information about the rank of $E(F)$. We now show a very simple example of this assertion which is a corollary of the Mordell–Weil Theorem.

Corollary 3.1.2. *Let K be an imaginary quadratic field of class number 1 with ring of integers $\mathcal{O}$. Suppose that E has complex multiplication by $\mathcal{O}$ and let $\alpha \in \mathcal{O}$ be an endomorphism. If $E(F)/\alpha E(F) = 0$, then $E(F)$ is finite.*

Proof. By the Mordell–Weil Theorem, $E(F)$ is a finitely generated $\mathbb{Z}$-module, and since $E(F)$ has complex multiplication by $\mathcal{O}$, it is a finitely generated $\mathcal{O}$-module. Using that K has class number one, the result follows from the structure theorem of finitely generated modules over a principal ideal domain. □

We proceed to explain how to study the group $E(F)/\alpha E(F)$. We have the following exact sequence of G_F-modules

$$0 \to E[\alpha] \to E(\bar{F}) \xrightarrow{\alpha} E(\bar{F}) \to 0.$$

Taking G_F-cohomology leads to a long exact sequence, where we only write the first terms

$$0 \to E[\alpha](F) \to E(F) \xrightarrow{\alpha} E(F) \xrightarrow{\delta} H^1(F, E[\alpha]) \to H^1(F, E) \xrightarrow{\alpha} H^1(F, E),$$

where $E = E(\bar{F})$ and δ is the connecting morphism

$$\delta : E(F) \to H^1(F, E[\alpha]), \quad P \mapsto [\sigma \mapsto Q^\sigma - Q] \text{ for some } Q \text{ satisfying } \alpha Q = P.$$

From this sequence we can obtain the following short exact sequence

$$0 \to E(F)/\alpha E(F) \xrightarrow{\delta} H^1(F, E[\alpha]) \to H^1(F, E)[\alpha] \to 0$$

(note that $H^1(F, E)$ is an $\mathrm{End}(E)$-module and $H^1(F, E)[\alpha]$ denotes the α-torsion of it).

We will study $E(F)/\alpha E(F)$ by studying its image by δ in $H^1(F, E[\alpha])$. As we will see, this would be easier if F were a local field. This motivates the following: fix a prime $\mathfrak{Q}$ (finite or infinite) of F and consider that E is defined over $F_{\mathfrak{Q}}$, repeating the same process we did for E/F but now with $E/F_{\mathfrak{Q}}$ we obtain the short exact sequence

$$0 \to E(F_{\mathfrak{Q}})/\alpha E(F_{\mathfrak{Q}}) \to H^1(F_{\mathfrak{Q}}, E[\alpha]) \to H^1(F_{\mathfrak{Q}}, E)[\alpha] \to 0.$$

And using that $F \subset F_{\mathfrak{Q}}$, and $G_F \supset G_{F_{\mathfrak{Q}}}$ we have the natural inclusion map

$$E(F)/\alpha E(F) \to E(F_{\mathfrak{Q}})/\alpha E(F_{\mathfrak{Q}})$$

and the restriction maps

$$H^1(F, E[\alpha]) \xrightarrow{\text{res}_{\mathfrak{Q}}} H^1(F_{\mathfrak{Q}}, E[\alpha]), \quad H^1(F, E) \xrightarrow{\text{res}_{\mathfrak{Q}}} H^1(F_{\mathfrak{Q}}, E).$$

We can consider these maps for every prime $\mathfrak{Q}$ of F to obtain the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(F)/\alpha E(F) & \xrightarrow{\delta} & H^1(F, E[\alpha]) & \longrightarrow & H^1(F, E)[\alpha] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_{\mathfrak{Q}} E(F_{\mathfrak{Q}})/\alpha E(F_{\mathfrak{Q}}) & \xrightarrow{\delta} & \prod_{\mathfrak{Q}} H^1(F_{\mathfrak{Q}}, E[\alpha]) & \longrightarrow & \prod_{\mathfrak{Q}} H^1(F_{\mathfrak{Q}}, E)[\alpha] & \longrightarrow & 0. \end{array}$$

Instead of studying the image of $E(F)/\alpha E(F)$, we will consider a larger group that is easier to characterize.

Definition 3.1.3. With the notation as above define the α-Selmer group of E/F as

$$\begin{aligned} S_\alpha(E_{/F}) &= \left\{ c \in H^1(F, E[\alpha]) : \text{res}_{\mathfrak{Q}}(c) \in \delta\left(E(F_{\mathfrak{Q}})/\alpha E(F_{\mathfrak{Q}})\right) \text{ for all } \mathfrak{Q} \right\} \\ &= \left\{ c \in H^1(F, E[\alpha]) : \text{res}_{\mathfrak{Q}}(c) = 0 \in H^1(F_{\mathfrak{Q}}, E) \text{ for all } \mathfrak{Q} \right\}. \end{aligned}$$

Remark 3.1.4. One can think of the Selmer group $S_\alpha(E_{/F})$ as the smallest group defined by natural local conditions containing $\delta(E(F)/\alpha E(F))$.

3.2 Some lemmas about cohomology

We state some lemmas that will be useful in the next sections. Let E be an elliptic curve defined over F, a field of characteristic 0, and suppose that E has complex multiplication by $\mathcal{O}$.

Lemma 3.2.1. *Let $\mathfrak{p}$ be a prime of K above $p > 3$. Let C be a subgroup of $(\mathcal{O}/\mathfrak{p}^n)^\times$ acting on $\mathcal{O}/\mathfrak{p}^n$ via multiplication. If C is not a p-group or C is cyclic, then for all $i > 0$*

$$H^i(C, \mathcal{O}/\mathfrak{p}^n) = 0.$$

Lemma 3.2.2. *Let $\mathfrak{p}$ be a prime of K lying above $p > 3$. Let $n \geq 0$:*

1. *If $\mathcal{O}_{\mathfrak{p}} = \mathbb{Z}_p$, or if $E[\mathfrak{p}] \not\subset E(F)$, the restriction map gives an isomorphism*

$$H^1(F, E[\mathfrak{p}^n]) \cong H^1(F(E[\mathfrak{p}^n]), E[\mathfrak{p}^n])^{\text{Gal}(F(E[\mathfrak{p}^n])/F)}.$$

2. *Suppose F is a finite extension of $\mathbb{Q}_\ell$ for some $\ell \neq p$. Then the restriction map gives an injection*

$$H^1(F, E)[\mathfrak{p}^n] \hookrightarrow H^1(F(E[\mathfrak{p}^n]), E)[\mathfrak{p}^n].$$

Lemma 3.2.3. *Suppose E is defined over K (i.e. $F = K$). Let $\mathfrak{p}$ be a prime of K not dividing 6 of good reduction. For $n \geq 1$ denote $K_{n,\mathfrak{p}} = K_{\mathfrak{p}}(E[\mathfrak{p}^n])$. Then the restriction map gives an injection*

$$H^1(K_{\mathfrak{p}}, E[\mathfrak{p}^n]) \hookrightarrow H^1(K_{n,\mathfrak{p}}, E[\mathfrak{p}^n]).$$

Proof. The kernel of the map is $H^1(K_{n,\mathfrak{p}}/K_{\mathfrak{p}}, E[\mathfrak{p}^n])$. Since the extension $K(E[\mathfrak{p}^n])/K$ is totally ramified at $\mathfrak{p}$ with Galois group $(\mathcal{O}/\mathfrak{p}^n)^\times$ (Theorem 2.6.4 (2) and (4)), we deduce that $\mathrm{Gal}(K_{n,\mathfrak{p}}/K_{\mathfrak{p}}) \cong (\mathcal{O}/\mathfrak{p}^n)^\times$ and acts on $E[\mathfrak{p}] \cong \mathcal{O}/\mathfrak{p}^n$ via multiplication. Since $(\mathcal{O}/\mathfrak{p}^n)^\times$ has order $\mathrm{N}\mathfrak{p}^{n-1}(\mathrm{N}\mathfrak{p}-1)$, so it is not a p-group, we can apply Lemma 3.2.1 to see $H^1(K_{n,\mathfrak{p}}/K, E[\mathfrak{p}^n]) = 0$ and we are done. □

3.3 The enlarged Selmer group

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}$. Let F be a finite extension of K with ring of integers $\mathcal{O}_F$. Consider E an elliptic curve defined over F with complex multiplication by $\mathcal{O}$. Let $\alpha \in \mathcal{O}$ such that $\alpha\mathcal{O} = \mathfrak{p}^n$ for some prime ideal $\mathfrak{p} \nmid 6$ and $n \geq 1$. Let p be the rational prime below $\mathfrak{p}$. If it is clear from the context we will write $\alpha \in \mathrm{End}(E)$ instead of $[\alpha]$.

As we explained in the first section, the α-Selmer group of E is defined by local conditions. In this section we focus on the local conditions at the primes $\mathfrak{Q}$ of F not dividing α. We do it by studying the following group.

Definition 3.3.1. Define the enlarged Selmer group of α as

$$\begin{aligned} S'_\alpha(E_{/F}) &= \left\{c \in H^1(F, E[\alpha]) : \mathrm{res}_{\mathfrak{Q}}(c) \in \delta\left(E(F_{\mathfrak{Q}})/\alpha E(F_{\mathfrak{Q}})\right) \text{ for all } \mathfrak{Q} \nmid \alpha\right\} \\ &= \left\{c \in H^1(F, E[\alpha]) : \mathrm{res}_{\mathfrak{Q}}(c) = 0 \in H^1(F_{\mathfrak{Q}}, E) \text{ for all } \mathfrak{Q} \nmid \alpha\right\}. \end{aligned}$$

Clearly, $S_\alpha(E_{/F}) \subset S'_\alpha(E_{/F})$.

Lemma 3.3.2. *Suppose that $E[\mathfrak{p}^n] \subset F$. Then*

$$S'_\alpha(E_{/F}) = \mathrm{Hom}(\mathrm{Gal}(M/F), E[\mathfrak{p}^n])$$

where M is the maximal abelian extension of F unramified outside primes above $\mathfrak{p}$.

Proof. Let $\mathfrak{Q}$ be a prime of F not dividing $\mathfrak{p}$. Since $E[\mathfrak{p}^n]$ is fixed by G_F

$$H^1(F, E[\mathfrak{p}^n]) = \mathrm{Hom}(G_F, E[\mathfrak{p}^n]), \quad H^1(F_{\mathfrak{Q}}, E[\mathfrak{p}^n]) = \mathrm{Hom}(G_{F_{\mathfrak{Q}}}, E[\mathfrak{p}^n])$$

($E[\mathfrak{p}^n]$ is finite, therefore all the homomorphisms are continuous in the profinite topology). From these observations, the enlarged Selmer group can be written as

$$S'_\alpha(E_{/F}) = \{c \in \mathrm{Hom}(G_F, E[\mathfrak{p}^n]) : \mathrm{res}_{\mathfrak{Q}}(c) \in \delta\left(E(F_{\mathfrak{Q}})/\alpha E(F_{\mathfrak{Q}})\right) \text{ for all } \mathfrak{Q} \nmid \alpha\}$$

and we have to study $\delta\left((E(F_{\mathfrak{Q}})/\alpha E(F_{\mathfrak{Q}})\right)$ in $\mathrm{Hom}(G_{F_{\mathfrak{Q}}}, E[\mathfrak{p}^n])$.

Since $E[\mathfrak{p}^n] \subset F_{\mathfrak{Q}}$ and $p > 3$, by Theorem 2.6.5 E has good reduction at $\mathfrak{Q}$. This means that we can apply Proposition 1.4.5 to note that the image of the connecting morphism δ is in

$$E(F_{\mathfrak{Q}})/\alpha E(F_{\mathfrak{Q}}) \xrightarrow{\delta} \mathrm{Hom}(G_{F_{\mathfrak{Q}}}/I_{\mathfrak{Q}}, E[\mathfrak{p}^n]), \tag{3.1}$$

where $I_{\mathfrak{Q}}$ is the intertia subgroup of $G_{F_{\mathfrak{Q}}}$. By local class field theory, $G_{F_{\mathfrak{Q}}}/I_{\mathfrak{Q}} \cong \hat{\mathbb{Z}}$, therefore

$$\mathrm{Hom}(G_{F_{\mathfrak{Q}}}/I_{\mathfrak{Q}}, E[\mathfrak{p}^n]) = \mathrm{Hom}(\hat{\mathbb{Z}}, E[\mathfrak{p}^n]) = \mathrm{Hom}(\mathbb{Z}, E[\mathfrak{p}^n]) \cong E[\mathfrak{p}^n] \cong \mathcal{O}/\mathfrak{p}^n.$$

On the other hand, the reduction map gives the following epimorphism

$$E(F_{\mathfrak{Q}}) \to \tilde{E}(k)/\alpha\tilde{E}(k),$$

where k is the residual field of $F_{\mathfrak{Q}}$. If $P \in E(F_{\mathfrak{Q}})$ is in the kernel of this map, $\tilde{P} = \tilde{\alpha}\tilde{R}$ for some $R \in E(F_{\mathfrak{Q}})$, i.e. $P - \alpha R \in E_1(F)$. And now, using that α is an isomorphism of $E_1(F_{\mathfrak{Q}})$ (see proof of Proposition 1.4.5) $P - \alpha R = \alpha R'$ with $R' \in E_1(F)$. From here it is clear that

$$E(F_{\mathfrak{Q}})/\alpha E(F_{\mathfrak{Q}}) \cong \tilde{E}(k)/\alpha\tilde{E}(k) \cong \mathcal{O}/\mathfrak{p}^n.$$

The last isomorphism comes from the fact that $\tilde{E}(k)$ is an elliptic curve with a finite number of points containing $E[\mathfrak{p}^m]$ for some $m \geq n$.

These observations show that the map in (3.1) is an isomorphsim. Hence

$$S'_\alpha(E_{/F}) = \{c \in \mathrm{Hom}(G_F, E[\mathfrak{p}^n]) : \mathrm{res}_{\mathfrak{Q}}(c) \in \mathrm{Hom}(G_{F_{\mathfrak{Q}}}/I_{\mathfrak{Q}}, E[\mathfrak{p}^n]) \text{ for all } \mathfrak{Q} \nmid \alpha\}$$

and the result follows. □

We are interested in finding $S'_\alpha(E_{/K})$ when E is defined over K. In this case we will not necessarily have $E[\mathfrak{p}^n] \subset E(K)$ but combining Lemma 3.3.2 with the results of the previous section we get the desired result.

Theorem 3.3.3. *Suppose E is defined over K (i.e. $F = K$). If we denote by $K_n = K(E[\mathfrak{p}^n])$*

$$S'_\alpha(E_{/K}) \cong \mathrm{Hom}(M_n/K_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}.$$

Here M_n is the maximal abelian extension of K_n unramified outside primes above $\mathfrak{p}$.

Proof. Since $p > 3$ one can check that the conditions of Lemma 3.2.2 (1) are satisfied: either p splits, which implies that $\mathcal{O}_{\mathfrak{p}} = \mathbb{Z}_p$ or if p does not split it is plain to see that we can apply Corollary 2.6.2 to ensure $E[\mathfrak{p}] \not\subset E(K)$. Therefore the restriction map

$$\phi : H^1(K, E[\mathfrak{p}^n]) \to H^1(K_n, E[\mathfrak{p}^n])$$

induces an isomorphism

$$H^1(K, E[\mathfrak{p}^n]) \cong H^1(K_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}.$$

Thus, we just need to see that

$$\phi\left(S'_\alpha(E_{/K})\right) = S'_\alpha(E_{/K_n})^{\mathrm{Gal}(K_n/K)}$$

and apply Lemma 3.3.2. To prove $\phi\left(S'_\alpha(E_{/K})\right) \subset S'_\alpha(E_{/K_n})^{\mathrm{Gal}(K_n/K)}$ let $c \in S'_\alpha(E_{/K})$ then, $\phi(c) \in H^1(K_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K))}$ so we are left to prove that $\phi(c) \in S'_\alpha(E_{/K_n})$. This is true because, if $\mathfrak{Q}$ is a prime of K_n not dividing α, and $\mathfrak{q}$ is the prime of K below it

$$\mathrm{res}_{\mathfrak{Q}}(\phi(c)) = \mathrm{res}_{\mathfrak{q}} c|_{G_{K_{n\mathfrak{Q}}}}.$$

For the other inclusion, if $c \in S'_\alpha(E_{/K_n})^{\mathrm{Gal}(K_n/K)} \subset H^1(K_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}$ it can be extended to $c \in H^1(K, E[\mathfrak{p}^n])$. Let $\mathfrak{q}$ be a prime of K not dividing $\mathfrak{p}$ and $\mathfrak{Q}$ a prime of K_n above $\mathfrak{q}$. Lemma 3.2.2 (2) implies that we have an injection

$$H^1(K_{\mathfrak{q}}, E)[\mathfrak{p}^n] \hookrightarrow H^1(K_{n\mathfrak{Q}}, E)[\mathfrak{p}^n]$$

which maps $\mathrm{res}_{\mathfrak{q}}(c) \mapsto \mathrm{res}_{\mathfrak{Q}}(c) = 0$, because $c \in S'_\alpha(E_{/K_n})$. By the injectivity, $\mathrm{res}_{\mathfrak{q}}(c) = 0$ in $H^1(K_{\mathfrak{q}}, E)$ and we are done. □

3.4 The Selmer group

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}$. Assume that K has class number 1. Let E be an elliptic curve defined over K with complex multiplication by $\mathcal{O}$. Let ψ be the Hecke character of attached to E with conductor $\mathfrak{f}$. Let $\mathfrak{p}$ be a prime of K coprime to $6\mathfrak{f}$ and let $\pi \in \mathcal{O}$ such that $\pi\mathcal{O} = \mathfrak{p}$. Finally, let $n \geq 1$.

The goal of the section is to study $\delta(E(K_{\mathfrak{p}})/\pi^n E(K_{\mathfrak{p}})$ in $H^1(K_{\mathfrak{p}}, E[\mathfrak{p}^n])$ and use it together with Theorem 3.3.3 to obtain the expression for the π^n-Selmer group for E/K.

Since $\mathfrak{p}$ is coprime to $\mathfrak{f}$, E has good reduction at $\mathfrak{p}$. Moreover, $v(p) \leq 2 < p-1$ so the logarithm map gives an isomorphism

$$\log_E : E_1(K_{\mathfrak{p}}) \xrightarrow{\sim} \mathfrak{p}\mathcal{O}_{\mathfrak{p}}.$$

Lemma 3.4.1. *1. There is a natural isomorphism*

$$E(K_{\mathfrak{p}}) \cong E_1(K_{\mathfrak{p}}) \times \tilde{E}(k).$$

2. The logarithm map extends to a surjective map $\log_E : E(K_\mathfrak{p}) \to \mathfrak{p}\mathcal{O}_\mathfrak{p}$ *whose kernel is finite and has no* $\mathfrak{p}$*-torsion.*

Proof. 1. Since E/K has good reduction at $\mathfrak{p}$, we have the exact sequence of $\mathcal{O}$-modules.

$$0 \to E_1(K_\mathfrak{p}) \to E(K_\mathfrak{p}) \to \tilde{E}(k) \to 0, \tag{3.2}$$

where k is the residue field of $K_\mathfrak{p}$.

The endomorphism $\psi(\mathfrak{p}) \in \mathcal{O}$ reduces to the Frobenius endomorphism of $\tilde{E}(k)$ (Proposition 2.5.11). This is an inseparable endomorphism and hence injective. Therefore $\tilde{E}(k)$ has no $\mathfrak{p}$-torsion (recall that $\psi(\mathfrak{p})\mathcal{O} = \mathfrak{p}$). On the other hand, the logarithm map gives $E_1(K_\mathfrak{p}) \cong \mathfrak{p}\mathcal{O}_\mathfrak{p}$. Using this two observations we can deduce that the exact sequence (3.2) splits. Indeed, if we write

$$\tilde{E}(k) \cong \bigoplus_i \mathcal{O}/(a_i),$$

where $a_i \in \mathcal{O}$ are coprime to $\mathfrak{p}$, we can use the properties of the Ext functor, which we will denote by Ext

$$\mathrm{Ext}(\oplus_i \mathcal{O}/(a_i), E_1(K_\mathfrak{p})) \cong \prod_i \mathrm{Ext}(\mathcal{O}/(a_i), E_1(K_\mathfrak{p})) \cong \prod_i E_1(K_\mathfrak{p})/a_i E_1(K_\mathfrak{p}) = 0$$

and we are done.

2. The desired map is defined by taking the logarithm $\log_E : E_1(K_\mathfrak{p}) \to \mathfrak{p}\mathcal{O}_\mathfrak{p}$ and compose it with the natural projection of the first coordinate

$$E_1(K_\mathfrak{p}) \times \tilde{E}(k) \to E_1(K_\mathfrak{p}).$$

□

Definition 3.4.2. There is an action of $\mathcal{O}_\mathfrak{p}$ on $E_1(K_\mathfrak{p})$ given by

$$\mathcal{O}_\mathfrak{p} \times E_1(K_\mathfrak{p}) \to E_1(K_\mathfrak{p}), \quad a, P \mapsto aP = \log_E^{-1}\left(a \log_E(P)\right).$$

Lemma 3.4.3. *If* $\alpha \in \mathcal{O} \subset \mathcal{O}_\mathfrak{p}$ *and* $P \in E_1(K_\mathfrak{p})$*, then* $\alpha P = [\alpha]P$*, where* $[\alpha] \in \mathrm{End}(E)$*.*

Proof. Given the endomorphism $[\alpha]$ consider its corresponding power series $[\alpha](T) = \alpha T + O(T^2)$. Recall the isomorphism

$$E_1(K_\mathfrak{p}) \to \hat{E}(\mathfrak{p}), \quad (x, y) \mapsto -x/y$$

and note that if $(x,y) \in E_1(K_\mathfrak{p})$, $[\alpha](x,y) \mapsto [\alpha](-x/y)$. From Corollary 1.2.5 we have

$$\alpha\omega(T) = \omega \circ [\alpha], (T)$$

where $\omega(T)$ is the invariant differential of the formal group $\hat{E}(\mathfrak{p})$. Integrating with respect to T and adjusting the constant

$$\alpha \log_{\hat{E}}(T) = \log_{\hat{E}}([\alpha]T).$$

Thus, denoting $P = (x,y)$ and $z = -x/y$ we have

$$\alpha P = \log_E^{-1}(\alpha \log_E(P)) = \log_E^{-1}(\alpha \log_{\hat{E}}(z)) = \log_E^{-1}(\log_{\hat{E}}([\alpha](z))) = [\alpha]P.$$

□

Remark 3.4.4. Recall the definitions of $\log_{\hat{E}} : \hat{E}(\mathfrak{p}) \xrightarrow{\sim} \mathfrak{p}\mathcal{O}_\mathfrak{p}$ and $\log_E : E_1(K_\mathfrak{p}) \xrightarrow{\sim} \hat{E}(\mathfrak{p}) \xrightarrow{\sim} \mathfrak{p}\mathcal{O}_\mathfrak{p}$.

As we did before, denote by $K_{n,\mathfrak{p}}$ the finite extension $K_\mathfrak{p}(E[\mathfrak{p}^n])$. This can be identified with the completion of $K_n = E[\mathfrak{p}^n]$ at the prime above $\mathfrak{p}$ (Theorem 2.6.4 (4) ensures K_n/K is totally ramified at $\mathfrak{p}$). Denote by $\mathcal{O}_{n,\mathfrak{p}}$ the ring of integers of $K_{n,\mathfrak{p}}$.

Note that the connecting morphism δ restricted to $G_{K_{n,\mathfrak{p}}}$ is essentially the following Kummer pairing

Definition 3.4.5. Define the following Kummer pairing

$$\langle\ ,\ \rangle_{\pi^n} : E(K_\mathfrak{p}) \times K_{n,\mathfrak{p}}^\times \to E[\mathfrak{p}^n], \quad P, x \mapsto \langle P, x\rangle_{\pi^n} = Q^{[x,K_{n,\mathfrak{p}}]} - Q,$$

where $Q \in E(\bar{K}_\mathfrak{p})$ is such that $\pi^n Q = P$ and $[\cdot, K_{n,\mathfrak{p}}]$ is the local Artin map.

Lemma 3.4.6. *Let $P \in E_1(K_\mathfrak{p})$, $x \in K_{n,\mathfrak{p}}^\times$ and $a \in \mathcal{O}_\mathfrak{p}$. Then*

$$\langle aP, x\rangle_{\pi^n} = a\langle P, x\rangle_{\pi^n}.$$

Remark 3.4.7. There is a natural action of $\mathcal{O}_\mathfrak{p}$ on $E[\mathfrak{p}^n]$: given $a \in \mathcal{O}_\mathfrak{p}$ and $P \in E[\mathfrak{p}^n]$, there exists $\alpha \in \mathcal{O}$ such that $a \equiv \alpha \mod \mathfrak{p}^n$. Then we define $aP = [\alpha]P$. This does not depend on the choice of α since $E[\mathfrak{p}]$ is an $\mathcal{O}/\mathfrak{p}$-module.

Proof. We will start by proving the proposition when $a = \alpha \in \mathcal{O} \cong \mathrm{End}(E)$. In this case, by Lemma 3.4.3 the statement can be rewritten as

$$\langle [\alpha]P, x\rangle_{\pi^n} = [\alpha]\langle P, x\rangle_{\pi^n}.$$

Let $Q \in E(\bar{K}_{\mathfrak{p}})$ such that $\pi^n Q = P$. Then, since $\mathrm{End}(E) \cong \mathcal{O}$ is commutative, $\pi^n \circ [\alpha]Q = [\alpha]P$. Hence

$$\langle [\alpha]P, x\rangle_{\pi^n} = ([\alpha]Q)^{[x,K_{n,\mathfrak{p}}]} - [\alpha]Q = [\alpha]Q^{[x,K_{n,\mathfrak{p}}]} - [\alpha]Q = [\alpha]\langle P, x\rangle_{\pi^n}$$

where we used that E is defined over K and therefore so is $[\alpha]$ (Proposition 2.3.1).

To complete the proof for the general case it is enough to show that if $a, b \in \mathcal{O}_{\mathfrak{p}}$ satisfy $a \equiv b \mod \mathfrak{p}^n$ then $\langle aP, x\rangle_{\pi^n} = \langle bP, x\rangle_{\pi^n}$, in other words, if $a \equiv 0 \mod \mathfrak{p}^n$ then $\langle aP, x\rangle_{\pi^n} = 0$. Suppose that $a \in \mathfrak{p}^n\mathcal{O}_{\mathfrak{p}}$, then $\log_E(aP) = a\log_E(P) = u\pi^{n+1} = \pi^n(u\pi)$ for some $u \in \mathcal{O}_{\mathfrak{p}}$. But since the logarithm $\log_E : E_1(K_{\mathfrak{p}}) \xrightarrow{\sim} \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ is an isomorphism, there exists $P' \in E_1(K_{\mathfrak{p}})$ such that

$$\log_E(aP) = \pi^n \log_E(P') \implies aP = \pi^n P'.$$

Using Lemma 3.4.3 we conclude that $aP = [\pi^n]P'$ so $\langle P, x\rangle_{\pi^n} = 0$ because P' is defined over $K_{\mathfrak{p}} \subset K_{n,\mathfrak{p}}$. □

Proposition 3.4.8. *There exists a unique Galois equivariant morphism $\delta_n : K_{n,\mathfrak{p}}^{\times} \to E[\mathfrak{p}^n]$ such that for any $P \in E(K_{\mathfrak{p}})$ and $x \in K_{n,\mathfrak{p}}^{\times}$*

$$\langle P, x\rangle_{\pi^n} = \left(\pi^{-1}\log_E(P)\right)\delta_n(x).$$

Proof. Let $R \in E_1(K_{\mathfrak{p}})$ such that $\log_E(R) = \pi$. It is plain to see that the only possibility is $\delta_n(x) = \langle R, x\rangle_{\pi^n}$ for all $x \in K_{n,\mathfrak{p}}^{\times}$ so the uniqueness is clear.

We need to prove that this map satisfies the desired condition. By Lemma 3.4.1 (1) and its proof we have that $E(K_{\mathfrak{p}}) \cong E_1(K_{\mathfrak{p}}) \times \tilde{E}(k)$. Hence, using the linearity of the Kummer pairing it is enough to prove the condition for each factor of the cartesian product.

If $P \in E_1(K_{\mathfrak{p}})$, it is easy to see that $P = \pi^{-1}\log_E(P)R$. So the equallity follows from the $\mathcal{O}_{\mathfrak{p}}$-equivariance of Proposition 3.4.6. If $P \in E(K_{\mathfrak{p}})$ is a torsion point, it has order prime to $\mathfrak{p}$ and hence $\langle P, x\rangle_{\pi^n} = 0$ which agrees with $\log_E(P) = 0$ (Lemma 3.4.1 (2)) so we are done.

Now we proceed to prove the Galois equivariance of δ_n. Let $x \in K_{n,\mathfrak{p}}^{\times}$ and $\sigma \in \mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{ab}}/K_{\mathfrak{p}})$. We need to see that

$$\langle R, x\rangle_{\pi^n}{}^{\sigma} = \langle R, x^{\sigma}\rangle_{\pi^n}. \tag{3.3}$$

If we let $Q \in E(\bar{K}_{\mathfrak{p}})$ such that $[\pi^n]Q = R$, we can rewrite (3.3) as

$$\left(Q^{[x,K_{n,\mathfrak{p}}]} - Q\right)^{\sigma} = Q^{[x^{\sigma},K_{n,\mathfrak{p}}]} - Q$$

By local class field theory this can be rewritten as

$$\left(Q^{[x,K_{n,\mathfrak{p}}]} - Q\right)^{\sigma} = Q^{\sigma^{-1}[x,K_{n,\mathfrak{p}}]\sigma} - Q.$$

Applying σ^{-1} in both sides and rearranging terms, the previous equallity holds if

$$Q - Q^{\sigma^{-1}} \in E(K_{n,\mathfrak{p}}).$$

And this is true because

$$[\pi^n](Q - Q^{\sigma^{-1}}) = P - P^{\sigma^{-1}} = P - P = 0 \implies Q - Q^{\sigma^{-1}} \in E[\mathfrak{p}^n] \subset E(K_{n,\mathfrak{p}}).$$

□

Proposition 3.4.9. *The map δ_n is surjective. In addition, $\delta_n(\mathcal{O}_{n,\mathfrak{p}}^\times) = E[\mathfrak{p}^n]$.*

Proof. We have the following injections

$$E(K_\mathfrak{p})/\mathfrak{p}^n E(K_\mathfrak{p}) \hookrightarrow H^1(K_\mathfrak{p}, E[\mathfrak{p}^n]) \hookrightarrow H^1(K_{n,\mathfrak{p}}, E[\mathfrak{p}^n]) \cong \mathrm{Hom}(K_{n,\mathfrak{p}}^\times, E[\mathfrak{p}^n]) \quad (3.4)$$

the first one by the connecting morphism and the second one by Lemma 3.2.3. The last isomorphism follows from $E[\mathfrak{p}^n] \subset E(K_{n,\mathfrak{p}})$ and local class field theory.

Suppose that $\delta_n(K_{n,\mathfrak{p}}^\times) \subset E[\mathfrak{p}^{n-1}]$, then Proposition 3.4.8 says that the image of $E(K_\mathfrak{p})/\mathfrak{p}^n E(K_\mathfrak{p})$ in $\mathrm{Hom}(K_{n,\mathfrak{p}}^\times, E[\mathfrak{p}^n])$ is a subset of $\mathrm{Hom}(K_{n,\mathfrak{p}}^\times, E[\mathfrak{p}^{n-1}])$, and hence every element would have order $\mathfrak{p}^{n-1}$. On the other hand, Lemma 3.4.1 (1) implies that $E(K_\mathfrak{p})/\mathfrak{p}^n E(K_\mathfrak{p}) \cong \mathcal{O}/\mathfrak{p}^n$ that has elements of exact order $\mathfrak{p}^n$, which contradicts the injectivity of the maps in (3.4). Hence $\delta_n(K_{n,\mathfrak{p}}^\times) \not\subset E[\mathfrak{p}^{n-1}]$, but by the galois equivariance of δ_n, the image $\delta_n(K_{n,\mathfrak{p}}^\times)$ has to be $G_{K_\mathfrak{p}}$-stable which implies that $\delta_n(K_{n,\mathfrak{p}}^\times) = E[\mathfrak{p}^n]$.

Similarly, since the Galois group $G_{K_\mathfrak{p}}$ acts trivially on $K_{n,\mathfrak{p}}^\times/\mathcal{O}_{n,\mathfrak{p}}^\times$, it has to act trivially on $\delta_n(K_{n,\mathfrak{p}}^\times)/\delta_n(\mathcal{O}_{n,\mathfrak{p}}^\times)$ so it must be equal to a quotient of $E[\mathfrak{p}^n]$ where $G_{K_\mathfrak{p}}$ acts trivially. The only possibility is that $\delta(\mathcal{O}_{n,\mathfrak{p}}^\times) = E[\mathfrak{p}^n]$ and we are done. □

Remark 3.4.10. In this proof we used that the extension $K(E[\mathfrak{p}^n])/K$ is totally ramified at $\mathfrak{p}$ with galois group $(\mathcal{O}/\mathfrak{p}^n)^\times$ which acts on $E[\mathfrak{p}^n] \cong \mathcal{O}/\mathfrak{p}^n$ via multiplication (see Theorem 2.6.4 (2) and (4)).

Theorem 3.4.11. *Let $K_n = K(E[\mathfrak{p}^n])$ with idele group $\mathbb{A}_{K_n}^\times$. Define*

$$W_n = K_n^\times \prod_{v|\infty} K_{n,v}^\times \prod_{v\nmid\mathfrak{p}\infty} \mathcal{O}_{n,v}^\times \cdot \ker \delta_n.$$

Then

$$S_{\pi^n}(E_{/K}) \cong \mathrm{Hom}(\mathbb{A}_{K_n}^\times/W_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}.$$

Proof. By Theorem 3.3.3 and class field theory

$$S'_{\pi^n}(E_{/K}) \cong \mathrm{Hom}\left(\mathbb{A}_{K_n}^{\times}/W'_n, E[\mathfrak{p}^n]\right)^{\mathrm{Gal}(K_n/K)}.$$

with $W'_n = K_n^{\times}\prod_{v|\infty} K_{n,v}^{\times}\prod_{v\nmid\mathfrak{p}\infty}\mathcal{O}_{n,v}^{\times}$. Hence, in order to find $S_{\pi^n}(E_{/K})$ we need to see which of these homomorphisms correspond to elements $c \in H^1(K, E[\mathfrak{p}^n])$ such that $\mathrm{res}_{\mathfrak{p}}(c) \in \delta(E(K_{\mathfrak{p}})/\pi^n E(K_{\mathfrak{p}}))$. Note that, looking more closely at the injections of the maps in (3.4) and recalling that δ_n is Galois equivariant one can determine the image

$$E(K_{\mathfrak{p}})/\mathfrak{p}^n E(K_{\mathfrak{p}}) \hookrightarrow \mathrm{Hom}(K_{n,\mathfrak{p}}^{\times}/\ker\delta_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}.$$

In fact, this is an isomorphism, because $K_{n,\mathfrak{p}}/\ker\delta_n \cong E[\mathfrak{p}^n]$ and using the Galois equivariance of δ_n

$$\mathrm{Hom}(K_{n,\mathfrak{p}}^{\times}/\ker\delta_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)} = \mathrm{Hom}(E[\mathfrak{p}^n], E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}$$

But using that $E[\mathfrak{p}^n] \cong \mathcal{O}/\mathfrak{p}^n$ and that $\mathrm{Gal}(K_n/K) \cong (\mathcal{O}/\mathfrak{p}^n)^{\times}$ acts via multiplication it is plain to see that

$$\mathrm{Hom}(E[\mathfrak{p}^n], E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)} \cong \mathrm{Hom}_{(\mathcal{O}/\mathfrak{p}^n)^{\times}}(\mathcal{O}/\mathfrak{p}^n, \mathcal{O}/\mathfrak{p}^n) \cong \mathrm{Hom}_{(\mathcal{O}/\mathfrak{p}^n)}(\mathcal{O}/\mathfrak{p}^n, \mathcal{O}/\mathfrak{p}^n)$$

and the last is isomorphic to $\mathcal{O}/\mathfrak{p}^n$. But we already saw in the previous proof that $E(K_{\mathfrak{p}})/\mathfrak{p}^n E(K_{\mathfrak{p}}) \cong \mathcal{O}/\mathfrak{p}^n$ so we have the isomorphism

$$E(K_{\mathfrak{p}})/\pi^n E(K_{\mathfrak{p}}) \cong \mathrm{Hom}(K_{n,\mathfrak{p}}^{\times}/\ker\delta_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}.$$

Therefore, we can write the following expression for the π^n-Selmer group

$$S_{\pi^n}(E_{/K}) \cong \Big\{ f \in \mathrm{Hom}(\mathbb{A}_{K_n}^{\times}/W'_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)} : \\ : \mathrm{res}_{K_{n,\mathfrak{p}}^{\times}} f \in \mathrm{Hom}(K_{n,\mathfrak{p}}^{\times}/\ker\delta_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)} \Big\}$$

which proves the theorem. □

For the proof of the Coates–Wiles Theorem it will be enough to focus on the case $n = 1$. To ease notation let $\Delta = \mathrm{Gal}(K_1/K)$. Define also ε to be the set of global units of K_1 and A the ideal class group of K_1. We have the following characterization.

Corollary 3.4.12. *The Selmer group $S_{\pi}(E_{/K}) = 0$ if and only if*

$$\mathrm{Hom}(A, E[\mathfrak{p}])^{\Delta} = 0 \text{ and } \delta_1(\varepsilon) \neq 0.$$

Proof. Denoting by $\bar{\varepsilon}$ the clousure of ε in $\mathcal{O}_{1,\mathfrak{p}}^{\times}$ and $V = \ker \delta_1 \cap \mathcal{O}_{1,\mathfrak{p}}^{\times}$ we have the inclusion

$$\mathcal{O}_{1,\mathfrak{p}}^{\times}/V\bar{\varepsilon} \hookrightarrow \mathbb{A}_{K_1}^{\times}/W_1.$$

On the other hand there is a natural isomorphism

$$\mathbb{A}_{K_1}^{\times}/K_1^{\times}U_1 \xrightarrow{\sim} A,$$

where $U_1 = \prod_{v|\infty} K_{1,v}^{\times} \prod_{v\nmid\infty} \mathcal{O}_{1,v}^{\times}$. This isomorphism sends $x \in \mathbb{A}_K^{\times}$ to the class of the ideal generated by x. Putting this together we get a Δ-equivariant exact sequence

$$0 \to \mathcal{O}_{1,\mathfrak{p}}^{\times}/V\bar{\varepsilon} \to \mathbb{A}_{K_1}^{\times}/W_1 \to A' \to 0,$$

where A' is a quotient of A by some power of the prime $\mathfrak{P}$ of K_1 above $\mathfrak{p}$. Moreover, considering the exact sequence obtained applying $\mathrm{Hom}(-, E[\mathfrak{p}])$ and taking the terms fixed by Δ we can conclude

$$\mathrm{Hom}(\mathbb{A}_{K_1}^{\times}/W_1, E[\mathfrak{p}])^{\Delta} = 0 \iff \mathrm{Hom}(A', E[\mathfrak{p}])^{\Delta} = 0 \text{ and } \mathrm{Hom}(\mathcal{O}_{1,\mathfrak{p}}^{\times}/V\bar{\varepsilon}, E[\mathfrak{p}])^{\Delta} = 0.$$

Note that, since $\mathfrak{P}$ has order divisible by $\mathrm{N}\mathfrak{p} - 1$ (which is coprime to $\#E[\mathfrak{p}] = \mathrm{N}\mathfrak{p}$), every element $c \in \mathrm{Hom}(A, E[\mathfrak{p}])$ factors through A modulo the class of $\mathfrak{P}$, in particular it factors through A'. From here

$$\mathrm{Hom}(A', E[\mathfrak{p}])^{\Delta} = 0 \iff \mathrm{Hom}(A, E[\mathfrak{p}])^{\Delta} = 0.$$

Now we will see that $\mathrm{Hom}(\mathcal{O}_{1,\mathfrak{p}}^{\times}/V\bar{\varepsilon}, E[\mathfrak{p}])^{\Delta} = 0$ is equivalent to $\delta_1(\varepsilon) \neq 0$. Suppose that $\delta_1(\varepsilon) = 0$, then $\bar{\varepsilon} \subset V$, so $\delta_1 : \mathcal{O}_{1,\mathfrak{p}}^{\times}/V \xrightarrow{\sim} E[\mathfrak{p}]$ gives a nonzero Δ-equivariant morphism. For the other implication, if $\delta(\varepsilon) \neq 0$, since ε is Δ-stable, $\delta(\varepsilon) = E[\mathfrak{p}]$. From here, it is plain to deduce that $\mathcal{O}_{1,\mathfrak{p}}^{\times} = V\varepsilon$ which shows that $\mathrm{Hom}(\mathcal{O}_{1,\mathfrak{p}}^{\times}/V\bar{\varepsilon}, E[\mathfrak{p}])^{\Delta} = 0$. □

3.5 The χ-isotypical component of the ideal class group

Continue with the notation of the previous section but assume that p splits in K. Recall that in the previous corollary we saw $S_\pi(E_{/K}) = 0$ if and only if

$$\mathrm{Hom}(A, E[\mathfrak{p}])^{\Delta} = 0 \text{ and } \delta_1(\varepsilon) \neq 0.$$

In this section we find an alternative way to write the first condition: it will be in terms of the so called isotypical component of the p part of A with respect to a

character. This will motivate part of the work that will be done in the next chapters. In addition, the definitions of the isotypical component of a module will be useful for the last chapters.

Recall that $\Delta = \mathrm{Gal}(K_1/K) \cong (\mathcal{O}/\mathfrak{p})^\times$ is a cyclic group of order $p-1$ (because p splits). Therefore all irreducible $\mathbb{F}_p$-representation of Δ are one dimensional and are determined by its character

$$\chi : \Delta \to \mathbb{F}_p^\times \hookrightarrow \mathbb{Z}_p^\times,$$

where we used Hensel's Lemma for the last inclusion. We are particularly interested in the following representation.

Definition 3.5.1. Define χ_E the $\mathbb{F}_p$-representation of Δ induced by the action of Δ on $E[\mathfrak{p}]$. It is one dimensional since $E[\mathfrak{p}]$ is a one dimensional $\mathbb{F}_p$-vector space (or also by 2.6.4 (2)).

The characterization that we will find is that the χ_E-isotypical component of the p part of A is is trivial. Let's recall the definition of this concept for any finitely generated Δ-module and then prove this statement.

Definition 3.5.2. Let M be a finitely generated Δ module, and hence a $\mathbb{Z}[\Delta]$-module. The p part of M is $M^{(p)} = M \otimes_{\mathbb{Z}} \mathbb{Z}_p$. This is a $\mathbb{Z}_p[\Delta]$-module.

Definition 3.5.3. Given a character χ of Δ with values in $\mathbb{Z}_p^\times$ define its idempotent, $\varepsilon(\chi) \in \mathbb{Z}_p[\Delta]$

$$\varepsilon(\chi) = \frac{1}{p-1} \sum_{\sigma \in \Delta} \chi(\sigma)^{-1} \sigma.$$

Now we can define the subgroup that we are interested in.

Definition 3.5.4. Given M a $\mathbb{Z}[\Delta]$-module and χ an irreducible representation of Δ with values in $\mathbb{Z}_p$ define $M^\chi = \varepsilon(\chi) M^{(p)}$. If $m \in M^{(p)}$ we will denote $m^\chi = \varepsilon(\chi) m$.

The next proposition should give a clear image of the submodule M^χ.

Proposition 3.5.5. *Let M be a $\mathbb{Z}[\Delta]$-module. Then:*

1. $M^\chi = \{m \in M^{(p)} : \sigma m = \chi(\sigma) m \text{ for all } \sigma \in \Delta\}$.
2. $M^{(p)} = \bigoplus_\chi M^\chi$, *where the sum is over all the irreducible representations of* Δ.

Proof. 1. Clear.

2. Note that

$$\sum_{\chi} \varepsilon(\chi) = 1 \tag{3.5}$$

where the sum is over all irreducible representations and $1 \in \Delta$ is the idenetity element. To prove (3.5) we just have to note that for every character $\psi : \Delta \to \mathbb{Z}_p$

$$\psi\left(\sum_{\chi} \varepsilon(\chi)\right) = \sum_{\chi} \frac{1}{p-1} \sum_{\sigma \in \Delta} \chi(\sigma)^{-1}\psi(\sigma) = 1$$

which follows from the orthonormality of the characters. Hence, if $m \in M^{(p)}$

$$m = \sum_{\chi} \varepsilon(\chi) m$$

and this proves that every element of $M^{(p)}$ can be written as sum of elements of M^{χ}.

To prove that the sum is direct suppose that it is not, and consider a nontrivial expression with the least number of nonzero terms:

$$\sum_{\chi} m^{\chi} = 0. \tag{3.6}$$

There are at least two characters, which we will denote as χ_0 and χ_1 for which the corresponding summands are nonzero. Choose $\sigma \in \Delta$ such that $\chi_0(\sigma) \neq \chi_1(\sigma)$. Applying $\sigma \in \Delta$ on both sides

$$\sum_{\chi} \chi(\sigma) m^{\chi} = 0 \tag{3.7}$$

But on the other hand, multiplying (3.6) by $\chi_0(\sigma)$ and substrating with (3.7) yields to another nontrivial expression with less nonzero terms than the original one. This is a contradiction.

□

Corollary 3.5.6. *If $P \in E[\mathfrak{p}]$, $P^{\chi_E} = P$, i.e. $E[\mathfrak{p}]^{\chi_E} = E[\mathfrak{p}]$.*

Proof. This is clear because $E[\mathfrak{p}] = E[\mathfrak{p}] \otimes \mathbb{Z}_p$ and χ_E is defined as the irreducible representation given by the action of Δ on $E[\mathfrak{p}]$ so the result follows from Proposition 3.5.5 (1). □

Now we can apply these definition to the case we are interested in. The Galois group Δ acts on A giving it a structure of a $\mathbb{Z}[\Delta]$-module. So we can consider A^{χ}.

Proposition 3.5.7. *The isotypical component* $A^{\chi_E} = 0$ *if and only if* $\mathrm{Hom}(A, E[\mathfrak{p}])^{\Delta} = 0$.

Proof. Assume there exists a nonzero $f \in \mathrm{Hom}(A, E[\mathfrak{p}])^{\Delta}$. Since the order of $E[\mathfrak{p}]$ is p, the restriction of $f \in \mathrm{Hom}(A^{(p)}, E[\mathfrak{p}])^{\Delta}$ has to be nonzero. Choose an element $\mathfrak{c} \in A^{(p)}$ such that $f(\mathfrak{c}) = P \neq 0$. By Corollary 3.5.6 we have that $\varepsilon(\chi_E)P = P$. Combining this with the Δ-equivariance of f

$$f(\mathfrak{c}^{\chi_E}) = f(\mathfrak{c})^{\chi_E} = P \neq 0.$$

Therefore, the restriction of f in A^{χ_E} is nonzero. Hence $A^{\chi_E} = 0$ and we are done.

For the other implication, if $A^{\chi_E} \neq 0$ it is plain to see that there is a nontrivial $\mathbb{Z}_p$-linear map between A^{χ_E} and $E[\mathfrak{p}]$. This is a nonzero element of $\mathrm{Hom}(A^{\chi_E}, E[\mathfrak{p}])^{\Delta}$. Now using that $A^{(p)} = \oplus_{\chi} A^{\chi}$ and $A = \oplus_q A^{(q)}$, where the last sum is over primes q, it is clear that we can extend this map to a nontrivial element of $\mathrm{Hom}(A, E[\mathfrak{p}])^{\Delta}$. $\square$

Chapter 4

Elliptic units

Fix K an imaginary quadratic field with ring of integers $\mathcal{O}$. Suppose that K has class number 1. The elliptic units of an elliptic curve E with complex multiplication by $\mathcal{O}$ are units of certain abelian extensions of K satisfying some norm-compatibility relations. They are defined as a product of some rational functions that depend essentially on the x-coordinates evaluated at certain of torsion points of E.

The importance of elliptic units on the Coates–Wiles Theorem is that they form an Euler system. As we will see, Euler systems can be used to give a bound of A^{χ_E}, where A is the ideal class group of $K(E[\mathfrak{p}])$ for a prime $\mathfrak{p}$ of K (see Definition 3.5.1 for the definition of χ_E). This is essential since showing that this subgroup is trivial is one of the conditions to ensure that the π-Selemer group of E is trivial (Proposition 3.5.7), where π is an $\mathcal{O}$-generator of $\mathfrak{p}$, which is our ultimate goal.

In this chapter we introduce the basic functions that will allow us to define the elliptic units. After that, we prove some relations between these functions that are essentially the norm-compatibility relations of the system of units. This will allow us to construct the Euler system of elliptic units in the chapter of Euler systems. We follow [Rub99] Chapter 7.

For this chapter fix E an elliptic curve defined over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$. Fix an ideal $\mathfrak{a}$ of $\mathcal{O}$ coprime to 6.

4.1 The rational functions $\Theta_{E,\mathfrak{a}}$ and $\Lambda_{E,\mathfrak{a}}$

We start by defining a rational function $\Theta_{E,\mathfrak{a}}$, finding its field of definition in terms of the field of definition of E and showing for which points P, $\Theta_{E,\mathfrak{a}}(P)$ is a unit.

After that we define $\Lambda_{E,\mathfrak{a}}$, a rational function obtained by taking products of translates of $\Theta_{E,\mathfrak{a}}$. This is the rational function that will produce the elliptic units.

Definition 4.1.1. Choose a Weierstrass equation for E and denote by $\Delta(E)$ its

discriminant. Let $\gamma \in \mathcal{O}$ a generator of the ideal $\mathfrak{a}$. Define

$$\Theta_{E,\mathfrak{a}} = \gamma^{-12}\Delta(E)^{\mathrm{N}\mathfrak{a}-1} \prod_{P \in E[\mathfrak{a}]-O} (x - x(P))^{-6}.$$

Remark 4.1.2. The fact that K is quadratic imaginary implies that the group of units of $\mathcal{O}^\times$ has order dividing 12. Therefore $\Theta_{E,\mathfrak{a}}$ does not depend on the choice of the generator γ of $\mathfrak{a}$.

Proposition 4.1.3. *The function $\Theta_{E,\mathfrak{a}}$ satisfies:*

1. *It does not depend on the Weierstrass equation for E.*
2. *If E' is an elliptic curve defined over $\mathbb{C}$ such that $\phi : E \to E'$ is an isomorphism, then $\Theta_{E,\mathfrak{a}} = \Theta_{E',\mathfrak{a}} \circ \phi$.*
3. *Let F be a subfield of $\mathbb{C}$. If E is defined over F, then $\Theta_{E,\mathfrak{a}}$ is defined over F.*

Proof. 1. Suppose that E is given by a Weierstrass equation with coordinate functions x, y. Choose another Weierstrass equation for E, this means choosing coordinates functions $x', y' \in K(E)$ such that

$$x' = u^2x + r, \quad y' = u^3y + sx + t \tag{4.1}$$

for $u \in \mathbb{C}^\times$ and $r, s, t \in \mathbb{C}$. Let E' be the curve defined by the Weierstrass equation corresponding to the coordinate functions x', y' (clearly it is isomorphic to E). We need to prove that

$$\Theta_{E,\mathfrak{a}} = \Theta_{E',\mathfrak{a}}.$$

Using that $\Delta(E') = u^{12}\Delta(E)$ and the fact that $\#E[\mathfrak{a}] = \mathrm{N}\mathfrak{a}$ we have

$$\begin{aligned}\Theta_{E',\mathfrak{a}} = \gamma^{-12}\Delta(E')^{\mathrm{N}\mathfrak{a}-1} \prod_{P \in E[\mathfrak{a}]-O} (x' - x'(P))^{-6} = \\ = \gamma^{-12}u^{12(\mathrm{N}\mathfrak{a}-1)}\Delta(E)^{\mathrm{N}\mathfrak{a}-1} \prod_{P \in E[\mathfrak{a}]-O} \left(u^2x - u^2x(P)\right)^{-6} = \Theta_{E,\mathfrak{a}}.\end{aligned}$$

2. This follows from (1): we just need to consider the Weierstrass equations for E and E', and since the two curves are isomorphic, the chosen coordinate functions of each curve will satisfy the relations of (4.1).

3. Notice that each automorphism $\sigma \in \mathrm{Gal}(E/F)$ fixes γ (because $K \subset F$) and fixes $\Delta(E)$ since E is defined over F. In addition σ permutes the elements of $E[\mathfrak{a}]$ and $O \in E[\mathfrak{a}](K)$ is fixed. The result follows.

□

Now that we know the field of definition of $\Theta_{E,\mathfrak{a}}$, it is easy to find the finite extension where $\Theta_{E,\mathfrak{a}}(Q)$ belongs when Q is a torsion point of E of order prime to $\mathfrak{a}$.

Proposition 4.1.4. *Let $\mathfrak{b}$ be a nontrivial ideal of $\mathcal{O}$ prime to $\mathfrak{a}$ and $Q \in E[\mathfrak{b}]$. Then $\Theta_{E,\mathfrak{a}}(Q) \in K(\mathfrak{b})$.*

Proof. Since K has class number 1, by Corollary 2.4.5 there exists E' defined over K isomorphic to E. Since the function $\Theta_{E,\mathfrak{a}}$ depends only on the isomorphism class of E (Proposition 4.1.3 (2)) we can suppose that E is defined over K. Moreover, Proposition 4.1.3 (3) shows that $\Theta_{E,\mathfrak{a}}$ is defined over K.

Let $U_{\mathfrak{b}} = \{x \in \mathbb{A}_K^\times : x_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^\times \text{ and } x_{\mathfrak{p}} \in 1 + \mathfrak{b}\mathcal{O}_{\mathfrak{p}} \text{ for all } \mathfrak{p}\}$. By class field theory we just need to see that if $x \in U_{\mathfrak{b}}$ then $\Theta_{E,\mathfrak{a}}(Q)$ is fixed by $[x, K]$. We clearly have

$$\Theta_{E,\mathfrak{a}}(Q)^{[x,K]} = \Theta_{E,\mathfrak{a}}\left(Q^{[x,K]}\right).$$

Now, we translate the action of $[x, K]$ on the $\mathfrak{b}$ torsion points to multiplication by $\alpha(x)x^{-1}$ where $\alpha(x) \in \mathcal{O}^\times$ (Proposition 2.5.1). But since $x \in U_{\mathfrak{b}}$, multiplication by x^{-1} is the identity. Hence,

$$\Theta_{E,\mathfrak{a}}\left(Q^{[x,K]}\right) = \Theta_{E,\mathfrak{a}}\left([\alpha(x)]Q\right) = \Theta_{E,\mathfrak{a}}\left(Q\right).$$

Where for the last equality we used again that $\Theta_{E,\mathfrak{a}}$ only depends on the isomorphism class of E and that $[\alpha]$ is an automorphism of E. □

We want to produce units with the rational function $\Theta_{E,\mathfrak{a}}$ by evaluating it at some torsion points. In order to do so, it is convenient to analyse the order of the term $(x(P) - x(Q))$ with respect all primes in function of the points $P, Q \in E$.

Lemma 4.1.5. *Suppose E is defined over K, $\mathfrak{p}$ a prime of K where E has good reduction. Fix a minimal Weierstrass equation of E with respect to $\mathfrak{p}$. Let $\mathfrak{b}, \mathfrak{c}$ be nontrivial ideals of $\mathcal{O}$ that are coprime. Consider $P \in E[\mathfrak{b}], Q \in E[\mathfrak{c}]$ two elements of exact order $\mathfrak{b}$ and $\mathfrak{c}$. Finally, fix an extension of the valuation at $\mathfrak{p}$ in $\bar{K}$ such that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{p}) = 1$.*

1. *If $\mathfrak{b} = \mathfrak{p}^n$, then $\mathrm{ord}_{\mathfrak{p}}(x(P)) = -2/\left(\mathrm{N}\mathfrak{p}^n - \mathrm{N}\mathfrak{p}^{n-1}\right)$.*
2. *If $\mathfrak{b}$ is not a power of $\mathfrak{p}$, then $\mathrm{ord}_{\mathfrak{p}}(x(P)) \geq 0$.*
3. *If $\mathfrak{p} \nmid \mathfrak{b}\mathfrak{c}$, then $\mathrm{ord}_{\mathfrak{p}}(x(P) - x(Q)) = 0$.*

Proof. 1. Let $F = K(E[\mathfrak{p}^n])$ and choose $\mathfrak{P}$ a prime of F above $\mathfrak{p}$. We are going to work with the local fields $F_{\mathfrak{P}}$ and $K_{\mathfrak{p}}$.

Now, write $\pi = \psi(\mathfrak{p})$, a generator of the ideal $\mathfrak{p}$. Hence $\ker([\pi]) = E[\mathfrak{p}]$. Also note that by Proposition 2.5.11, $[\pi]$ reduces to the $\mathrm{N}\mathfrak{p}$-Frobenius endomorphism

of the reduced curve $\tilde{E}(k)$ (k is the residue field of $K_\mathfrak{p}$), which is an inseparable endomorphism. From here it is plain to see that $[\pi^n]$ is an endomorphism of E with kernel $E[\mathfrak{p}^n]$ which reduces to the nth power of the N$\mathfrak{p}$-Frobenius, that is also inseparable. Therefore $E[\mathfrak{p}^n] \subset E_1(F_\mathfrak{P})$.

In order to find the valuation of $x(P)$ we will find the valuation of $z = -x(P)/y(P)$ by working with the formal group $\hat{E}(\mathfrak{P})$. We can do that because we just saw in the last paragraph that $P \in E_1(F_\mathfrak{P}) \cong \hat{E}(\mathfrak{P})$. Given the endomorphism $[\pi]$ consider its corresponding endomorphism of the formal group. It has the form

$$[\pi](Z) = \pi Z + O(Z^2) \in Z\mathcal{O}_\mathfrak{p}[[Z]].$$

And similarly, we have that for $[\pi^m]$ its corresponding endomorphism, $[\pi^m](T)$, is the composition of m times $[\pi](Z)$. Thus, it is easy to see that if we let

$$f(Z) = \frac{[\pi^n](Z)}{[\pi^{n-1}](Z)} = \frac{[\pi]\left([\pi^{n-1}](Z)\right)}{[\pi^{n-1}](Z)}.$$

we have $f(Z) \in \mathcal{O}_\mathfrak{p}[[Z]]$ and

$$f(Z) \equiv \pi \mod Z, \quad f(Z) \equiv Z^{\mathrm{N}\mathfrak{p}^n - \mathrm{N}\mathfrak{p}^{n-1}} \mod \mathfrak{p}\mathcal{O}_\mathfrak{p}[[Z]],$$

where the second congruence follows from the fact that the N$\mathfrak{p}$-Frobenius automorphism has corresponding power series $Z^{\mathrm{N}\mathfrak{p}}$. By the Weierstrass preparation theorem, there exists $u(Z) \in \mathcal{O}_\mathfrak{p}[[Z]]^\times$ and $e(Z) \in \mathcal{O}_\mathfrak{p}[Z]$ polynomial of degree $\mathrm{N}\mathfrak{p}^n - \mathrm{N}\mathfrak{p}^{n-1}$ such that $f(Z) = u(Z)e(Z)$. Reducing this equation modulo $\mathfrak{p}$ and using that $u(Z)$ is a unit we see that $e(Z)$ reduces to $Z^{\mathrm{N}\mathfrak{p}^n - \mathrm{N}\mathfrak{p}^{n-1}}$. Moreover, $f(Z) \equiv \pi \mod Z$. From these observations we conclude that $e(Z)$ is an Eisenstein polynomial.

Since P has order exactly $\mathfrak{p}^n$ we can evaluate $f(z) = [\pi^n](z)/[\pi^{n-1}](z) = 0$. Using that the valuation of z is positive and $u(Z)$ is a unit, $u(z) \neq 0$ so $e(z) = 0$. Thus, z is a root of an Eisenstein polynomial. It is known that the valuation of a root of this Eisenstein polynomial has to be $1/\left(\mathrm{N}\mathfrak{p}^n - \mathrm{N}\mathfrak{p}^{n-1}\right)$. The result follows from $z = -x(P)/y(P)$ and Proposition 1.3.6.

2. Let F be a finite extension of K such that $P \in E(F)$. Consider $\mathfrak{P}$ a prime of F above $\mathfrak{p}$. Then E as a curve defined over F has good reduction at $\mathfrak{P}$. Since the order of $P \in E[\mathfrak{b}]$ is not a power of $\mathfrak{p}$, by a similar argument than the one done in Corollary 1.1.9 and Proposition 1.4.1 (1) we have that $P \notin E_1(F_\mathfrak{P})$. Therefore we have that the valuation of $x(P) \in F_\mathfrak{P}$ has to be positive by Proposition 1.3.6.

3. Let F be a finite extension of K where P, Q are defined. Let $\mathfrak{P}$ be a prime of F above $\mathfrak{p}$. Since $\mathfrak{b}, \mathfrak{c}$ are not powers of $\mathfrak{p}$, by (2) we have that $\mathrm{ord}_\mathfrak{p}(x(P)), \mathrm{ord}_\mathfrak{p}(x(Q)) \geq$

0. Hence, $\mathrm{ord}_{\mathfrak{p}}(x(P)-x(Q)) \geq 0$. For the sake of contradiction suppose that $\mathrm{ord}_{\mathfrak{p}}(x(P)-x(Q)) > 0$, reducing the points modulo the prime above $\mathfrak{p}$ according the valuation $\mathrm{ord}_{\mathfrak{p}}$ we get $\widetilde{x(P)} = \widetilde{x(Q)}$. Using the definition of the reduction map we see that it has to be $x(\tilde{P}) = x(\tilde{Q})$, where this equality is of points of the reduced curve $\tilde{E}$. But by the addition law of points, if two points have the same x-coordinate it has to be $\tilde{P} \pm \tilde{Q} = \tilde{O}$. Since the reduction map is a morphism, we get that the point $P \pm Q \in E_1(F_{\mathfrak{P}})$, but $P \pm Q$ has order $\mathfrak{bc}$ that it is clearly not a power of $\mathfrak{p}$ so we get a contradiction because $E_1(F_{\mathfrak{P}})$ has no elements of order prime to $\mathfrak{p}$ (as we already said in (2)).

□

Using the observations of this last proposition it is possible to determine some torsion points Q for which $\Theta_{E,\mathfrak{a}}(Q)$ is a unit.

Theorem 4.1.6. *Suppose E is defined over K. Let $\mathfrak{b}$ be a nontrivial ideal of $\mathcal{O}$ prime to $\mathfrak{a}$. Take $Q \in E[\mathfrak{b}]$ an element of exact order $\mathfrak{b}$.*

1. *If $\mathfrak{b}$ is not a power of a prime, then $\Theta_{E,\mathfrak{a}}(Q) \in K(\mathfrak{b})$ is a global unit.*
2. *If $\mathfrak{b}$ is a power of $\mathfrak{p}$ for some prime of K, then $\Theta_{E,\mathfrak{a}}(Q) \in K(\mathfrak{b})$ is a local unit at all primes different from $\mathfrak{p}$.*

Proof. Let $\mathfrak{q}$ be a prime of K such that $\mathfrak{b}$ is not a power of $\mathfrak{q}$. Since $\Theta_{E,\mathfrak{a}}$ depends only on the isomorphism class, we can suppose that our Weierstrass equation for E has good reduction at $\mathfrak{q}$ (Proposition 2.6.5), i.e. $\Delta(E)$ is prime to $\mathfrak{q}$. Let $n = \mathrm{ord}_{\mathfrak{q}}(\mathfrak{a})$. Then

$$\mathrm{ord}_{\mathfrak{q}}(\Theta_{E,\mathfrak{a}}(Q))/6 = -2n - \sum_{P \in E[\mathfrak{a}]-O} \mathrm{ord}_{\mathfrak{q}}(x(Q)-x(P)) =$$
$$= -2n - \sum_{P \in E[\mathfrak{q}^n]-O} \mathrm{ord}_{\mathfrak{q}}(x(Q)-x(P)) - \sum_{P \in E[\mathfrak{a}]-E[\mathfrak{q}^n]} \mathrm{ord}_{\mathfrak{q}}(x(Q)-x(P)).$$

Now we use Lemma 4.1.5 to say:

- If P has exact order $\mathfrak{q}^m$, $m > 0$, then $\mathrm{ord}_{\mathfrak{q}}(x(Q)-x(P)) = -2/(\mathrm{N}\mathfrak{q}^m - \mathrm{N}\mathfrak{q}^{m-1})$.
- If P has order that is not a power of $\mathfrak{q}$ then $\mathrm{ord}_{\mathfrak{q}}(x(Q)-x(P)) = 0$.

Hence, we can compute

$$\mathrm{ord}_{\mathfrak{q}}(\Theta_{E,\mathfrak{a}}(Q))/6 = -2n - \sum_{m=1}^{n} \left(\sum_{P \in E[\mathfrak{q}^m]-E[\mathfrak{q}^{m-1}]} -2/\left(\mathrm{N}\mathfrak{q}^m - \mathrm{N}\mathfrak{q}^{m-1}\right) \right).$$

And $\#(E[\mathfrak{q}^m] - E[\mathfrak{q}^{m-1}]) = \mathrm{N}\mathfrak{q}^m - \mathrm{N}\mathfrak{q}^{m-1}$ so the result follows. □

We now introduce the function $\Lambda_{E,\mathfrak{a}}$ that will be used to produce the elliptic units. This function is defined as a product of some translates of $\Theta_{E,\mathfrak{a}}$. The motivation for this definition will be clear when we relate $\Theta_{E,\mathfrak{a}}$ with the L-series, since we will see that we need to consider different translates of $\Theta_{E,\mathfrak{a}}$ to obtain all the information of the L-series.

Definition 4.1.7. Suppose that E is defined over K. Let ψ be the Hecke character attached to E with conductor $\mathfrak{f}$. Let $S \in E$ be an $\mathcal{O}$-generator of $E[\mathfrak{f}]$. Define

$$\Lambda_{E,\mathfrak{a}} = \prod_{\sigma \in \mathrm{Gal}(K(\mathfrak{f})/K)} \Theta_{E,\mathfrak{a}} \circ \tau_{S^\sigma},$$

where $\tau_{S^\sigma}(P) = P + S^\sigma$ for every $P \in E$ is the translation by S^σ.

We have

Proposition 4.1.8. *Suppose that E is defined over K and let ψ be the Hecke character attached to E with conductor $\mathfrak{f}$:*

1. *The rational function $\Lambda_{E,\mathfrak{a}}$ is defined over K.*
2. *Suppose that $\mathfrak{r}$ is a nontrivial ideal of $\mathcal{O}$ coprime to $\mathfrak{f}$ and $Q \in E[\mathfrak{r}]$ has order exactly $\mathfrak{r}$. Then $\Lambda_{E,\mathfrak{a}}(Q)$ is a global unit in $K(E[\mathfrak{r}])$.*

Proof. 1. Any $\sigma' \in \mathrm{Aut}(\mathbb{C}/K)$ permutes the elements of $E[\mathfrak{f}]$. Combining this with the fact that $\Theta_{E,\mathfrak{a}}$ is defined over K (Proposition 4.1.3 (3)) leads to the desired result.

2. It is clear that $\Lambda_{E,\mathfrak{a}}(Q) \in K(E[\mathfrak{r}])$ because $\Lambda_{E,\mathfrak{a}}$ is defined over K. To see that it is a unit note that for any $\sigma \in \mathrm{Gal}(K(\mathfrak{f})/K)$, S^σ has order exaclty $\mathfrak{f}$. Therefore $Q + S^\sigma$ has order exactly $\mathfrak{r}\mathfrak{f}$ that it is not a power of a prime ($\mathfrak{f}$ is nontrivial by Corollary 2.6.1). Applying Theorem 4.1.6 (1) we obtain that $\Theta_{E,\mathfrak{a}}(Q+S^\sigma) \in K(\mathfrak{r}\mathfrak{f})$ is a global unit and hence $\Lambda_{E,\mathfrak{a}}(Q)$ is a unit for being a product of units.

□

The system of elliptic units consists of a system of units of the form $\Lambda_{E,\mathfrak{a}}(P)$ for some well chosen torsion points P. The way to choose these points will be explained in the chapter of Euler systems.

4.2 The distribution relation

The distribution relation is going to give us the norm compatibility relations of the Euler system of elliptic units. Since $\Lambda_{E,\mathfrak{a}}$ is a product of translates of $\Theta_{E,\mathfrak{a}}$, it is enough to prove the norm-compatibility relations for $\Theta_{E,\mathfrak{a}}$ because they will easily translate to $\Lambda_{E,\mathfrak{a}}$.

Lemma 4.2.1. *The function $\Theta_{E,\mathfrak{a}}$ is a rational function with divisor*

$$12\mathrm{N}\mathfrak{a}(O) - 12\sum_{P\in E[\mathfrak{a}]}(P)$$

Proof. Let $P \in E[\mathfrak{a}] - O$. The coordinate function x is a rational function, therefore so is $(x - x(P))^{-6}$. Thus, the product $\Theta_{E,\mathfrak{a}}$ is a rational function. To find its divisor we use that the divisor of $(x - x(P))$ is $(P) + (-P) - 2(O)$ and the formula for $\Theta_{E,\mathfrak{a}}$. □

Now we can prove the distribution relation.

Theorem 4.2.2 (Distribution relation)**.** *Suppose that E is defined over K. Let $\mathfrak{b}$ be a nontrivial ideal of $\mathcal{O}$ prime to $\mathfrak{a}$. Consider $\beta \in \mathcal{O}$ an $\mathcal{O}$-generator of $\mathfrak{b}$. Then, for any $P \in E(\mathbb{C})$.*

$$\prod_{R\in E[\mathfrak{b}]}\Theta_{E,\mathfrak{a}}(P+R) = \Theta_{E,\mathfrak{a}}(\beta P).$$

Proof. Lemma 4.2.1 allows us to compute the divisors of the two rational functions

$$\begin{aligned}\mathrm{div}\left(\prod_{R\in E[\mathfrak{b}]}\Theta_{E,\mathfrak{a}}(P+R)\right) &= \sum_{R\in E[\mathfrak{b}]}\mathrm{div}\left(\tau_R^*\Theta_{E,\mathfrak{a}}\right) = \sum_{R\in E[\mathfrak{b}]}\tau_R^*\mathrm{div}\left(\Theta_{E,\mathfrak{a}}\right) = \\ &= \sum_{R\in E[\mathfrak{b}]}\left(12\mathrm{N}\mathfrak{a}(-R) - 12\sum_{P\in E[\mathfrak{a}]}(P-R)\right) = 12\mathrm{N}\mathfrak{a}\sum_{R\in E[\mathfrak{b}]}(R) - 12\sum_{Q\in E[\mathfrak{a}\mathfrak{b}]}(Q),\end{aligned}$$

here τ_R denotes translation by R. Similarly

$$\begin{aligned}\mathrm{div}(\beta^*\Theta_{E,\mathfrak{a}}) = \beta^*\mathrm{div}(\Theta_{E,\mathfrak{a}}) &= \beta^*\mathrm{div}\left(12\mathrm{N}\mathfrak{a}(O) - 12\sum_{P\in E[\mathfrak{a}]}(P)\right) = \\ &= 12\mathrm{N}\mathfrak{a}\sum_{R\in E[\mathfrak{b}]}(R) - 12\sum_{P\in E[\mathfrak{a}]}\sum_{R\in\beta^{-1}P}(R) = 12\mathrm{N}\mathfrak{a}\sum_{R\in E[\mathfrak{b}]}(R) - 12\sum_{Q\in E[\mathfrak{a}\mathfrak{b}]}(Q),\end{aligned}$$

where we used that $\mathfrak{a}, \mathfrak{b}$ are relatively prime for both calculations. Since the two functions have the same divisors their ratio $\lambda \in K^\times$ is a constant. We compute λ by evaluating the ratio at $P = O$

$$\lambda = \frac{\prod_{R \in E[\mathfrak{b}]} \Theta_{E,\mathfrak{a}}(R)}{\Theta_{E,\mathfrak{a}}(\beta P)} = \frac{\Delta(E)^{(\mathrm{N}\mathfrak{a}-1)(\mathrm{N}\mathfrak{b}-1)}}{\gamma^{12(\mathrm{N}\mathfrak{b}-1)}\beta^{12(\mathrm{N}\mathfrak{a}-1)}} \prod_{\substack{R \in E[\mathfrak{b}]-O \\ P \in E[\mathfrak{a}]-O}} (x(R) - x(P))^{-6}.$$

Note that we have $\beta^{12(\mathrm{N}\mathfrak{a}-1)}$ in the denominator. This comes from evaluating the limit

$$\frac{x(O) - x(P)}{x(\beta O) - x(P)} = 1/\beta^2. \tag{4.2}$$

It can be justified using formal groups: consider the power series $x(Z) = Z^{-2} + \dots$ of (1.3) in terms of the uniformizer Z. Consider also the morphism $[\beta](Z) = \beta Z + O(Z^2)$. Substituting this in (4.2) and taking the limit when Z tends to 0 leads to the desired result. Proceeding as in the proof of Theorem 4.1.6 one can see that λ is a global unit of K, i.e. $\lambda \in \mathcal{O}^\times$. We will see that, if we let $\omega_K = \#\mathcal{O}^\times$, we can write $\lambda = \epsilon^{\omega_K}$ for some $\epsilon \in K^\times$. This implies that $\epsilon \in \mathcal{O}^\times$ and therefore $\lambda = 1$ as we want.

Let's show that such ϵ exists: since K is a quadratic imaginary extension of $\mathbb{Q}$ we have that $\omega_K \mid 12$. It is also true that $\omega_K \mid (\mathrm{N}\mathfrak{a} - 1)$ if $\mathfrak{a}$ is coprime to 6. This last assertion is clear when $\omega_K = 2$. Otherwise, if $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(\mu_3)$ one has to analyze when the rational primes that divide $\mathfrak{a}$ split or stay prime (note that since $\mathfrak{a}$ is coprime to 6 none of them ramify). Using also that x is an even function we can choose ϵ as

$$\epsilon = \frac{\Delta(E)^{(\mathrm{N}\mathfrak{a}-1)(\mathrm{N}\mathfrak{b}-1)/\omega_K}}{\gamma^{12(\mathrm{N}\mathfrak{b}-1)/\omega_K}\beta^{12(\mathrm{N}\mathfrak{a}-1)/\omega_K}} \prod_{\substack{R \in E[\mathfrak{b}]-O \\ P \in (E[\mathfrak{a}]-O)/\pm 1}} (x(R) - x(P))^{-12/\omega_K}$$

and we are done. □

Lemma 4.2.3. *Let $\mathfrak{b}$ be a nontrivial ideal of $\mathcal{O}$ prime to $\mathfrak{a}$ and $Q \in E[\mathfrak{b}]$ a point of exact order $\mathfrak{b}$. If $\mathfrak{c}$ is an ideal of $\mathcal{O}$ prime to $\mathfrak{b}$ and $\sigma_\mathfrak{c} = (\mathfrak{c}, K(\mathfrak{b})/K)$ we have*

$$\Theta_{E,\mathfrak{a}}(Q)^{\sigma_\mathfrak{c}} = \Theta_{E,\mathfrak{a}}(cQ)$$

where $c \in \mathcal{O}$ is an $\mathcal{O}$-generator of the ideal $\mathfrak{c}$ and $K(\mathfrak{b})$ is the ray class field of K modulo $\mathfrak{b}$.

Remark 4.2.4. We denote by $(\cdot, K(\mathfrak{b})/K)$ the Artin map in terms of ideals. On the other hand we denote by $[\cdot, K]$ the Artin map in terms of ideles.

Proof. Since $\Theta_{E,\mathfrak{a}}$ only depends on the isomorphism class of E we can suppose that E is defined over K. Thus, we need to compute $\Theta_{E,\mathfrak{a}}(Q^{\sigma_c})$. By class field theory, we can choose $x \in \mathbb{A}_K^\times$ a finite idele such that $x_\mathfrak{p} = 1$ for all $\mathfrak{p} \mid \mathfrak{b}$ and $(x) = \mathfrak{c}$ satisfying $[x, K]|_{K(\mathfrak{b})} = \sigma_\mathfrak{c}$.

Now we use Lemma 2.5.1 to translate the action of $[x, K]$ on Q as multiplication by $x^{-1}\alpha(x)$, where $\alpha(x)\mathcal{O} = \mathfrak{c}$. But since Q has order $\mathfrak{b}$, the map multiplication by x^{-1} is the identity on Q. Thus

$$\Theta_{E,\mathfrak{a}}(Q^{[x,K]}) = \Theta_{E,\mathfrak{a}}(\alpha(x)Q) = \Theta_{E,\mathfrak{a}}(cQ).$$

For the last equality we used that $\alpha(x) = uc$ for some unit $u \in \mathcal{O}^\times$ and that $\Theta_{E,\mathfrak{a}}$ only depends on the isomorphism class of E. □

The following is the expression of the distribution relation that we will use

Corollary 4.2.5. *Let $\mathfrak{b}$ be an ideal of $\mathcal{O}$ prime to $\mathfrak{a}$ and $Q \in E[\mathfrak{b}]$ of exact order $\mathfrak{b}$. Let $\mathfrak{p}$ be a prime dividing $\mathfrak{b}$ and $\pi \in \mathcal{O}$ such that $\pi\mathcal{O} = \mathfrak{p}$. Let $\mathfrak{b}' = \mathfrak{b}\mathfrak{p}^{-1}$ and suppose that it is a nontrivial ideal of $\mathcal{O}$. Then*

$$\mathrm{N}_{K(\mathfrak{b})/K(\mathfrak{b}')}\Theta_{E,\mathfrak{a}}(Q) = \begin{cases} \Theta_{E,\mathfrak{a}}(\pi Q) & \text{if } \mathfrak{p} \mid \mathfrak{b}' \\ \Theta_{E,\mathfrak{a}}(\pi Q)^{1-\mathrm{Frob}_\mathfrak{p}^{-1}} & \text{if } \mathfrak{p} \nmid \mathfrak{b}' \end{cases}$$

Where in the case $\mathfrak{p} \nmid \mathfrak{b}'$ we denote $\mathrm{Frob}_\mathfrak{p} = (\mathfrak{p}, K(\mathfrak{b}')/K)$.

Proof. As we have done before we can suppose that E is defined over K because K has class number 1, therefore $\Theta_{E,\mathfrak{a}}$ is defined over K.

For any integral ideal $\mathfrak{s}$ define $U_\mathfrak{s} = \left\{x \in \mathbb{A}_K^\times \mid x_\mathfrak{q} \in \mathcal{O}_\mathfrak{q}^\times \text{ and } x_\mathfrak{q} \in 1 + \mathfrak{s}\mathcal{O}_\mathfrak{q} \text{ for all } \mathfrak{q}\right\}$, from class field theory

$$[\,.\,, K] : \mathbb{A}_K^\times / \left(K^\times U_\mathfrak{s}\right) \xrightarrow{\sim} \mathrm{Gal}(K(\mathfrak{s})/K),$$

where $\mathfrak{s}$ is the ray class field of K modulo $\mathfrak{s}$. Considering the exact sequence

$$1 \to \mathrm{Gal}(K(\mathfrak{b})/K(\mathfrak{b}')) \to \mathrm{Gal}(K(\mathfrak{b})/K) \to \mathrm{Gal}(K(\mathfrak{b}')/K) \to 1$$

it is plain to deduce

$$\mathrm{Gal}(K(\mathfrak{b})/K(\mathfrak{b}')) \cong U_{\mathfrak{b}'}/U_\mathfrak{b} \cong U_\mathfrak{p}^{(n)}/U_\mathfrak{p}^{(n+1)}.$$

where $n = \mathrm{ord}_\mathfrak{p}(\mathfrak{b}')$ and $U_\mathfrak{p}^{(n)}$ equals the nth higher unit group if $n \geq 1$ and it equals to $\mathcal{O}_\mathfrak{p}^\times$ if $n = 0$.

We can compute the norm using this isomorphisms

$$\mathrm{N}_{K(\mathfrak{b})/K(\mathfrak{b}')}\Theta_{E,\mathfrak{a}}(Q) = \prod_{x\in U_{\mathfrak{p}}^{(n)}/U_{\mathfrak{p}}^{(n+1)}} \Theta_{E,\mathfrak{a}}(Q^{[x,K]})$$

where the product is done for a set of representatives of $U_{\mathfrak{p}}^{(n)}/U_{\mathfrak{p}}^{(n+1)}$. Now, by Lemma 2.5.1 we translate the action of $[x,K]$ to multiplication by $x^{-1}\alpha(x)$ on $\mathfrak{b}^{-1}L/L$, where L is a fractional ideal of $\mathcal{O}$ such that $f:\mathbb{C}/L \xrightarrow{\sim} E(\mathbb{C})$ is an isomorphism. Thus, letting $Q=f(t)$ and using that $\alpha(x)$ is an automorphism of E (because $(x)=\mathcal{O}=\alpha\mathcal{O}$)

$$\Theta_{E,\mathfrak{a}}(Q^{[x,K]}) = \Theta_{E,\mathfrak{a}}(\alpha(x)f(x^{-1}t)) = \Theta_{E,\mathfrak{a}}(f(x^{-1}t)).$$

To study the possibilities for $x^{-1}t$ write $t=(t_{\mathfrak{q}})$ with $t_{\mathfrak{q}} \in (\mathfrak{b}_{\mathfrak{q}})^{-1}L_{\mathfrak{q}}/L_{\mathfrak{q}}$ (we are using the isomorphism of Proposition 2.4.1). We have that $x\in\mathbb{A}_K^{\times}$ has 1 in all the components except at the $\mathfrak{p}$ component, where it has an element of $U_{\mathfrak{p}}^{(n)}$. Therefore x^{-1} only affects the $\mathfrak{p}$ component of $(t_{\mathfrak{q}})$

$$x^{-1}(t_{\mathfrak{q}}) = (x_{\mathfrak{q}}^{-1}t_{\mathfrak{q}}) = \begin{cases} t_{\mathfrak{q}} & \text{if } \mathfrak{q}\neq\mathfrak{p}, \\ x_{\mathfrak{p}}^{-1}t_{\mathfrak{p}} = t_{\mathfrak{p}} + t_{\mathfrak{p}}(x_{\mathfrak{p}}^{-1}-1) & \text{if } \mathfrak{q}=\mathfrak{p}. \end{cases} \tag{4.3}$$

This expression shows that we can write

$$f(x^{-1}t) = f(t) + f(t_{\mathfrak{p}}(x_{\mathfrak{p}}^{-1}-1)) = Q+R.$$

Using that t has exact order $\mathfrak{b}$ and that $x_{\mathfrak{p}}\in U_{\mathfrak{p}}^{(n)}$ we see that $R\in E[\mathfrak{p}]$. Moreover, from (4.3) it is also easy to see that the points R are distinct if the x are in different equivalence classes of $U_{\mathfrak{p}}^{(n)}/U_{\mathfrak{p}}^{(n+1)}$. Now we consider the following two cases:

- If $n\geq 1$, we have $\#\left(U_{\mathfrak{p}}^{(n)}/U_{\mathfrak{p}}^{(n+1)}\right) = \mathrm{N}\mathfrak{p} = \#E[\mathfrak{p}]$. Hence

$$\prod_{x\in U_{\mathfrak{p}}^{(n)}/U_{\mathfrak{p}}^{(n+1)}} \Theta_{E,\mathfrak{a}}(x^{-1}Q) = \prod_{R\in E[\mathfrak{p}]} \Theta_{E,\mathfrak{a}}(P+R) = \Theta_{E,\mathfrak{a}}(\pi P).$$

  Where we used the distribution relation of Theorem 4.2.2.

- If $n=0$, we have $\#\left(U_{\mathfrak{p}}^{(n)}/U_{\mathfrak{p}}^{(n+1)}\right) = \mathrm{N}\mathfrak{p}-1$. Let's see for which R_0 it is not possible that

$$x^{-1}Q = Q + R_0.$$

  Using (4.3) we notice that $x^{-1}t$ has order exactly $\mathfrak{b}$. Hence, it is not possible that $Q+R\in E[\mathfrak{b}']$. But certantly there exists exactly one $R_0\in E[\mathfrak{p}]$ such that

$Q + R_0$ has exact order $\mathfrak{b}'$ (it would correspond to $R_0 = f(-t_\mathfrak{p})$). Hence, using the distribution relation again

$$\mathrm{N}_{K(\mathfrak{b})/K(\mathfrak{b}')}\Theta_{E,\mathfrak{a}}(Q) = \prod_{R_0 \neq R \in E[\mathfrak{p}]} \Theta_{E,\mathfrak{a}}(P+R) = \Theta_{E,\mathfrak{a}}(\pi Q)/\Theta_{E,\mathfrak{a}}(Q+R_0).$$

And now we use that $Q + R_0 \in E[\mathfrak{b}']$ and that $\mathfrak{b}'$ is nontrivial by hypothesis, so we can apply Lemma 4.2.3 with $\mathrm{Frob}_\mathfrak{p} = (\mathfrak{p}, K(\mathfrak{b}')/K)$ to get

$$\Theta_{E,\mathfrak{a}}(Q+R_0)^{\mathrm{Frob}_\mathfrak{p}} = \Theta_{E,\mathfrak{a}}(\pi(Q+R_0)) = \Theta_{E,\mathfrak{a}}(\pi Q).$$

Applying $\mathrm{Frob}_\mathfrak{p}^{-1}$ on both sides we get the desired result.

□

Chapter 5

Euler systems

Let K be an imaginary quadratic field of class number 1. Denote by $\mathcal{O}$ its ring of integers.

In this chapter we give a general definition of an Euler system. Then we define the concrete case of elliptic units and show that it is an Euler system. After that, we explain how every unit of an Euler system generates a principal ideal of an extension of K. Moreover, we will find the factorizations of these ideals in terms of other units using the norm-compatibility relations, the so called Factorization Theorem. This theorem will give relations of the ideal class group which will be useful to bound its cardinality in the next chapter.

We essentially follow [Rub99] Chapter 8 except for the last section where we state and prove the Factorization Theorem following [CS06] Chapter 5. However, in [CS06] the proof is done for cyclotomic units. Therefore, some modifications have to be done using the so called universal Euler system. To study the universal Euler system we are doing a particular case of [Rub00] Chapter 4, Section 2. There, one can find the study of Euler systems in greater generality.

Fix an elliptic curve E defined over K with complex multiplication by $\mathcal{O}$. Let ψ be the Hecke character attached to E with conductor $\mathfrak{f}$. Choose a prime $\mathfrak{p}$ of K not dividing $6\mathfrak{f}$ and let p be the rational prime below it. Fix an ideal $\mathfrak{a}$ of $\mathcal{O}$ coprime to $6\mathfrak{p}\mathfrak{f}$. Let $\mathcal{R}$ be the set of square free ideals of $\mathcal{O}$ coprime to $6\mathfrak{f}\mathfrak{p}\mathfrak{a}$. Finally, for $n \geq 0$ denote by $K_n = K(E[\mathfrak{p}^n])$, if $\mathfrak{r} \in \mathcal{R}$ denote by $K_n(\mathfrak{r}) = K(E[\mathfrak{p}^n\mathfrak{r}])$ and let $G_\mathfrak{r} = \mathrm{Gal}(K_n(\mathfrak{r})/K_n)$.

5.1 The Euler system of elliptic units

We will work with the following definition of Euler system.

Definition 5.1.1. An Euler system is a set of global units

$$\left\{\eta(n,\mathfrak{r}) \in K_n(\mathfrak{r})^\times \mid n \geq 1 \text{ and } \mathfrak{r} \in \mathcal{R}\right\}$$

satsifying:

1. If $\mathfrak{rq} \in \mathcal{R}$, where $\mathfrak{q}$ is a prime ideal of $\mathcal{O}$, then

$$\mathrm{N}_{K_n(\mathfrak{rq})/K_n(\mathfrak{r})}\eta(n,\mathfrak{rq}) = \eta(n,\mathfrak{r})^{(1-\mathrm{Frob}_\mathfrak{q}^{-1})}.$$

2. If $\mathfrak{r} \in \mathcal{R}$ and $n \geq 1$, then

$$\mathrm{N}_{K_{n+1}(\mathfrak{r})/K_n(\mathfrak{r})}\eta(n+1,\mathfrak{r}) = \eta(n,\mathfrak{r}).$$

Remark 5.1.2. In the first equality we have that $\mathfrak{qr} \in \mathcal{R}$. Hence, $\mathrm{Frob}_\mathfrak{q} \in \mathrm{Gal}(K_n(\mathfrak{r})/K)$ is well defined because $K_n(\mathfrak{r}) = K(E[\mathfrak{p}^n\mathfrak{r}])$ and since $\mathfrak{p}^n\mathfrak{r}$ and $\mathfrak{q}$ are coprime the extension $K_n(\mathfrak{r})/K$ is unramified at $\mathfrak{q}$.

Using the functions defined in the previous chapter we now define a system of units and prove that it is an Euler system. We will call this system the Euler system of elliptic units. This is the system we are interested in. Fix an analytic isomorphism $\xi : \mathbb{C}/L \xrightarrow{\sim} E(\mathbb{C})$ where $L = \Omega\mathcal{O}$ and $\Omega \in \mathbb{C}$.

Definition 5.1.3. Given an integer $n \geq 0$ and an integral ideal $\mathfrak{r} \in \mathcal{R}$ define

$$\eta_n^{(\mathfrak{a})}(\mathfrak{r}) = \Lambda_{E,\mathfrak{a}}\left(\xi\left(\psi(\mathfrak{p}^n\mathfrak{r})^{-1}\Omega\right)\right).$$

Where the expression for $\Lambda_{E,\mathfrak{a}}$ is in Definition 4.1.7. The set $\{\eta_n^{(\mathfrak{a})}(\mathfrak{r})\}$ for $n \geq 1$ and $\mathfrak{r} \in \mathcal{R}$ is the set of elliptic units. We will sometimes omit the reference to $\mathfrak{a}$ and just write $\eta_n(\mathfrak{r})$.

Remark 5.1.4. Using that $\psi(\mathfrak{p}^n\mathfrak{r})$ generates the ideal $\mathfrak{p}^n\mathfrak{r}$ we see that $\eta_n(\mathfrak{r})$ is $\Lambda_{E,\mathfrak{a}}$ evaluated at the point $Q = \xi\left(\psi\left(\mathfrak{p}^n\mathfrak{r}\right)^{-1}\Omega\right)$ of exact order $\mathfrak{p}^n\mathfrak{r}$.

We proceed to find the fields of definition of these units as well as the compatibility relations between them.

Proposition 5.1.5. *For an integer $n \geq 1$ and integral ideal $\mathfrak{r} \in \mathcal{R}$, $\eta_n(\mathfrak{r})$ is a global unit in $K_n(\mathfrak{r})^\times$. Moreover:*

1. *If $\mathfrak{q} \in \mathcal{R}$ is a prime ideal such that $\mathfrak{qr} \in \mathcal{R}$. Then*

$$\mathrm{N}_{K_n(\mathfrak{rq})/K_n(\mathfrak{r})}\eta_n(\mathfrak{rq}) = \eta_n(\mathfrak{r})^{(1-\mathrm{Frob}_\mathfrak{q}^{-1})},$$

where $\mathrm{Frob}_\mathfrak{q} \in \mathrm{Gal}(K_n(\mathfrak{r})/K)$.

2. $\mathrm{N}_{K_{n+1}(\mathfrak{r})/K_n(\mathfrak{r})}\eta_{n+1}(\mathfrak{r}) = \eta_n(\mathfrak{r})$.

In other words, $\{\eta_n(\mathfrak{r})\}$ *with* $n \geq 1$ *and* $\mathfrak{r} \in \mathcal{R}$ *is an Euler system.*

Proof. As we mentioned in Remark 5.1.4, $\eta_n(\mathfrak{r}) = \Lambda_{E,\mathfrak{a}}(Q)$ for $Q = \xi\left(\psi(\mathfrak{p}^n\mathfrak{r})^{-1}\Omega\right)$ an $\mathcal{O}$-generator of $E[\mathfrak{p}^n\mathfrak{r}]$. Hence, we can apply Proposition 4.1.8 (1) and (3) to see that $\eta_n(\mathfrak{r}) \in K_n(\mathfrak{r})$ and that it is a global unit for $n \geq 1$. We proceed to prove the other two points:

1. By Theorem 2.6.4 (3) we can write

$$\mathrm{N}_{K_n(\mathfrak{rq})/K_n(\mathfrak{r})}\left(\eta_n(\mathfrak{rq})\right) = \mathrm{N}_{K(\mathfrak{fp}^n\mathfrak{rq})/K(\mathfrak{fp}^n\mathfrak{r})}\left(\eta_n(\mathfrak{rq})\right) = \mathrm{N}_{K(\mathfrak{fp}^n\mathfrak{rq})/K(\mathfrak{fp}^n\mathfrak{r})}\left(\Lambda_{E,\mathfrak{a}}(R)\right)$$

   where $R = \xi\left(\psi(\mathfrak{p}^n\mathfrak{rq})^{-1}\Omega\right) \in E[\mathfrak{p}^n\mathfrak{rq}]$. Now, using the expression of $\Lambda_{E,\mathfrak{a}}$ as a product of terms of the form $\Theta_{E,\mathfrak{a}}(R+S)$ with S of exact order $\mathfrak{f}$ we use Corollary 4.2.5 (2) to calculate

$$\mathrm{N}_{K(\mathfrak{fp}^n\mathfrak{rq})/K(\mathfrak{fp}^n\mathfrak{r})}\Theta_{E,\mathfrak{a}}(R+S) = \Theta(\pi R + \pi S)^{1-\mathrm{Frob}_{\mathfrak{q}}^{-1}} \tag{5.1}$$

   where $\pi \in \mathcal{O}$ is a generator of $\mathfrak{q}$. In fact, we can choose π such that $\pi\xi(\psi(\mathfrak{p}^n\mathfrak{qr})^{-1}\Omega) = \xi(\psi(\mathfrak{p}^n\mathfrak{r})^{-1}\Omega)$. In addition, since $\mathfrak{q}$ is coprime to $\mathfrak{f}$, π permutes the elements S of exact order $\mathfrak{f}$. Now the result follows multiplying (5.1) for all the elements S of exact order $\mathfrak{f}$.

2. The proof is the same than the proof of part (1) but in this case one has to use Corollary 4.2.5 (1).

□

5.2 The extensions $K_n(\mathfrak{r})$

Fix $n \geq 1$ a positive integer and $\mathfrak{r} \in \mathcal{R}$. Denote by $G_{\mathfrak{r}} = \mathrm{Gal}(K_n(\mathfrak{r})/K_n)$. The units of an Euler system lie in extensions of the form $K_n(\mathfrak{r})$. In this section we study these extensions, their Galois group and the ramification at some primes. Recall that we denote $G_{\mathfrak{r}} = \mathrm{Gal}(K_n(\mathfrak{r})/K_n)$.

Lemma 5.2.1. $G_{\mathfrak{r}} \cong (\mathcal{O}/\mathfrak{r})^{\times}$. *Similarly,* $\mathrm{Gal}(K_n(\mathfrak{r})/K_n(\mathfrak{rs}^{-1})) \cong (\mathcal{O}/\mathfrak{s})^{\times}$.

Proof. Consider the exact sequence

$$1 \to \mathrm{Gal}(K(E[\mathfrak{p}^n\mathfrak{r}])/K(E[\mathfrak{p}^n])) \to \mathrm{Gal}(K(E[\mathfrak{p}^n\mathfrak{r}])/K) \to \mathrm{Gal}(K(E[\mathfrak{p}^n])/K) \to 1.$$

The result follows from Theorem 2.6.4 (2) and the fact that $\mathfrak{r}$ and $\mathfrak{p}$ are coprime.

For the second assertion the proof is the same. □

Proposition 5.2.2. *Let $\mathfrak{q}$ be a prime such that $\mathfrak{q} \mid \mathfrak{r}$. Then $K_n(\mathfrak{r}\mathfrak{q}^{-1}) \cap K_n(\mathfrak{q}) = K_n$ and $K_n(\mathfrak{r}\mathfrak{q}^{-1})K_n(\mathfrak{q}) = K_n(\mathfrak{r})$.*

Proof. Observe that Theorem 2.6.4 (4) shows that $K_n(\mathfrak{q})/K_n$ is totally ramified at $\mathfrak{q}$. On the other hand, using that $\mathfrak{p}$ is coprime to 6 we have that the reduction map $\mathcal{O}^\times \to (\mathcal{O}/\mathfrak{p}^n)^\times$ is injective, and following a very similar reasoning that was done in the proof of Theorem 2.6.4 (5) we see that $K_n(\mathfrak{r}\mathfrak{q}^{-1})/K_n$ is unramified at $\mathfrak{q}$. Hence, $K_n(\mathfrak{q}) \cap K_n(\mathfrak{r}\mathfrak{q}^{-1}) = K_n$. Therefore, since all these extensions are Galois

$$[K_n(\mathfrak{r}\mathfrak{q}^{-1})K_n(\mathfrak{q}) : K(\mathfrak{r}\mathfrak{q}^{-1})] = [K_n(\mathfrak{q}) : K_n] = \mathrm{N}\mathfrak{q} - 1.$$

where we used Lemma 5.2.1 for the last equality. On the other hand, using again Lemma 5.2.1 we obtain

$$[K_n(\mathfrak{r}) : K_n(\mathfrak{r}\mathfrak{q}^{-1})] = \frac{[K_n(\mathfrak{r}) : K_n]}{[K_n(\mathfrak{r}\mathfrak{q}^{-1}) : K_n]} = \mathrm{N}\mathfrak{q} - 1,$$

because $\mathfrak{r}\mathfrak{q}^{-1}$ and $\mathfrak{q}$ are coprime. But it is clear that $K_n(\mathfrak{q})K_n(\mathfrak{r}\mathfrak{q}^{-1}) \subset K_n(\mathfrak{r})$ so the result follows. □

The next two corollaries are consequence of the previous Proposition and its proof.

Corollary 5.2.3. *Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}$ such that $\mathfrak{q} \mid \mathfrak{r}$. Every prime above $\mathfrak{q}$ in K_n is ramified of degree $\mathrm{N}\mathfrak{q} - 1$ in the extension $K_n(\mathfrak{r})/K_n$.*

Proof. See the proof of Proposition 5.2.2. □

Corollary 5.2.4. *We have*

$$G_{\mathfrak{r}} = \prod_{\mathfrak{q}\mid\mathfrak{r}} G_{\mathfrak{q}}$$

where the product is over prime ideals of $\mathcal{O}$ dividing $\mathfrak{r}$.

Proof. Apply Proposition 5.2.2 and induct on the number of primes dividing $\mathfrak{r}$. □

Remark 5.2.5. If $\mathfrak{r} \in \mathcal{R}$ and $\mathfrak{s} \mid \mathfrak{r}$ we will also denote by $G_{\mathfrak{s}} = \mathrm{Gal}(K_n(\mathfrak{r})/K_n(\mathfrak{r}\mathfrak{s}^{-1}))$.

5.3 Universal Euler system

We present an equivalent way to define an Euler system. Given $\mathfrak{r} \in \mathcal{R}$ and $n \geq 1$ we will represent the collection of units of the Euler system that lie in $K_n(\mathfrak{r})$ as indeterminate variables: for every $\mathfrak{s}$ such that $\mathfrak{s} \mid \mathfrak{r}$ we will consider the indeterminate $x_{n,\mathfrak{s}}$ to represent the unit of $K_n(\mathfrak{s})$. The elements of $\mathrm{Gal}(K_n(\mathfrak{r})/K)$ will act on the variables giving a structure of $\mathbb{Z}[\mathrm{Gal}(K_n(\mathfrak{r})/K)]$-module. We will define some relations

on this module in order to have the compatibility relations of an Euler system. Finally, taking the direct limit with respect to $\mathfrak{r}$ and n we will be able to consider all the units in extensions of the form $K_n(\mathfrak{r})$.

The reason why we need to give this definition is that the $\mathbb{Z}[\mathrm{Gal}(K_n(\mathfrak{r})/K)]$-module that is obtained doing this construction is torsion free. This will translate on having a canonical way to take the Mth root of an element (when it exists) which is necessary, as we will see in the next section, to define the principal ideals in K_n.

In the case of the Euler system of cyclotomic units it is not necessary to introduce this universal system because $\mathbb{Q}$ and the field extensions that are considered do not contain roots of unity of order greater than 2 (since these fields are totally real). In our case, both the base field K and its extensions can have nontrivial roots of unity so we need to work with the universal system.

We start defining the norm operator.

Definition 5.3.1. Given $\mathfrak{r} \in \mathcal{R}$, define

$$N_{\mathfrak{r}} = \sum_{\sigma \in G_{\mathfrak{r}}} \sigma \in \mathbb{Z}[G_{\mathfrak{r}}].$$

Note that $N_{\mathfrak{r}} = \prod_{\mathfrak{q}|\mathfrak{r}} N_{\mathfrak{q}}$.

We can now begin with the construction of the universal Euler system.

Definition 5.3.2. Let $\mathfrak{r} \in \mathcal{R}$ and $n \geq 1$, define $X_{n,\mathfrak{r}}$ the $\mathbb{Z}[\mathrm{Gal}(K_n(\mathfrak{r})/K)]$-module generated by the indeterminates $\{x_{n,\mathfrak{s}} : \mathfrak{s} \mid \mathfrak{r}\}$ modulo the relations:

1. If $\mathfrak{s} \mid \mathfrak{r}$ and $\sigma \in \mathrm{Gal}(K_n(\mathfrak{r})/K_n(\mathfrak{s}))$ we have $x_{n,\mathfrak{s}} = \sigma x_{n,\mathfrak{s}}$.
2. if $\mathfrak{q}\mathfrak{s} \mid \mathfrak{r}$, $N_{\mathfrak{q}} x_{n,\mathfrak{q}\mathfrak{s}} = (1 - \mathrm{Frob}_{\mathfrak{q}}^{-1}) x_{n,\mathfrak{s}}$, where $\mathrm{Frob}_{\mathfrak{q}} \in \mathrm{Gal}(K_n(\mathfrak{s})/K)$.

The next definition explains what is the universal Euler system and gives an equivalent way to define an Euler system using it.

Definition 5.3.3. The universal Euler system is

$$\varinjlim_{\mathfrak{r},n} X_{n,\mathfrak{r}}.$$

where the direct limit is taken over $\mathfrak{r} \in \mathcal{R}$ and $n \geq 1$.

Then, an Euler system is a Galois equivariant map

$$\eta : \varinjlim_{\mathfrak{r},n} X_{n,\mathfrak{r}} \to \bigcup_{\mathfrak{r},n} K_n(\mathfrak{r})^{\times}$$

such that $\eta(x_{n,\mathfrak{r}}) \in K_n(\mathfrak{r})^{\times}$ is a global unit.

We now study the structure of $X_{n,\mathfrak{r}}$. The following theorem is the reason we introduced the universal Euler system. To prove the theorem we will need the next lemma.

Lemma 5.3.4. *Let $\mathfrak{r} \in \mathcal{R}$ and $n \geq 1$. For every prime ideal $\mathfrak{q} \mid \mathfrak{r}$ and ideal $\mathfrak{s} \mid \mathfrak{r}$ define*

$$B_{\mathfrak{q}} = G_{\mathfrak{q}} - \{1\} \subset \mathbb{Z}[G_{\mathfrak{q}}], \quad B_{\mathfrak{s}} = \prod_{\mathfrak{q}|\mathfrak{s}} B_{\mathfrak{q}} \subset \mathbb{Z}[G_{\mathfrak{s}}].$$

In addition, let $A_1 \subset \mathrm{Gal}(K_n(\mathfrak{r})/K)$ be a complete set of representatives of $\mathrm{Gal}(K_n/K)$ and for every ideal $\mathfrak{s} \mid \mathfrak{r}$ define $A_{\mathfrak{s}} = A_1 B_{\mathfrak{s}}$. Then, the family

$$A = \bigcup_{\mathfrak{s}|\mathfrak{r}} A_{\mathfrak{s}} x_{n,\mathfrak{s}}$$

is a generating set of $X_{n,\mathfrak{r}}$ as a $\mathbb{Z}$-module.

Proof. Let $\sigma \in \mathrm{Gal}(K_n(\mathfrak{r})/K)$ and $\mathfrak{s} \mid \mathfrak{r}$. We need to see that the element $\sigma x_{n,\mathfrak{s}}$ can be written as a $\mathbb{Z}$-linear combination of elements of A. Let's prove it by induction on the number of primes dividing $\mathfrak{s}$. If $\mathfrak{s} = 1$, $\mathrm{Gal}(K_n(\mathfrak{r})/K)$ acts on $x_{n,1}$ through the quotient $\mathrm{Gal}(K_n/K)$. Since A_1 is a set of representatives of this quotient the result follows. Now let $\mathfrak{s} \mid \mathfrak{r}$ and suppose that the result is proven for all ideals with less prime factors than $\mathfrak{s}$. We can write $\sigma = \sigma'\tau$ with $\sigma' \in A_1$ and $\tau \in \mathrm{Gal}(K_n(\mathfrak{r})/K_n)$ so it is enough to prove that $\tau x_{n,\mathfrak{s}}$ can be writen as a linear combination of elements of A. If $\tau \in B_{\mathfrak{s}}$ we are done. Otherwise, there is $\mathfrak{q} \mid \mathfrak{s}$ prime such that $\tau = \tau_{\mathfrak{q}}\tau_{\mathfrak{s}/\mathfrak{q}}$ where $1 = \tau_{\mathfrak{q}} \in G_{\mathfrak{q}}$. Therefore

$$\tau x_{n,\mathfrak{s}} = \tau_{\mathfrak{s}/\mathfrak{q}}\tau_{\mathfrak{q}} x_{n,\mathfrak{s}} = \tau_{\mathfrak{s}/\mathfrak{q}} N_{\mathfrak{q}} x_{n,\mathfrak{s}} - \left(\tau_{\mathfrak{s}/\mathfrak{q}} \sum_{i=1}^{\mathrm{N}\mathfrak{q}-2} \sigma_{\mathfrak{q}}^i\right) x_{n,\mathfrak{s}}.$$

For the first term we can use that

$$\mathrm{N}_{\mathfrak{q}} x_{n,\mathfrak{s}} = \left(1 - \mathrm{Frob}_{\mathfrak{q}}^{-1}\right) x_{n,\mathfrak{s}/\mathfrak{q}}$$

and apply the induction hypothesis. For the second one we just have to repeat this process until we obtain an element of the form $\tau x_{n,\mathfrak{s}}$ with $\tau \in B_{\mathfrak{s}}$. □

Theorem 5.3.5. *If $\mathfrak{r} \in \mathcal{R}$ and $n \geq 1$ then $X_{n,\mathfrak{r}}$ is a free $\mathbb{Z}$-module.*

Proof. We will prove that the generating set A found in the lemma is a $\mathbb{Z}$-basis of $X_{n,\mathfrak{r}}$. It is easy to count the number of generators of A: using that $\#B_{\mathfrak{q}} = \mathrm{N}\mathfrak{q} - 2$ we have

$$\#A = \sum_{\mathfrak{s}|\mathfrak{r}} \#A_s = \#A_1 \sum_{\mathfrak{s}|\mathfrak{r}} \#B_{\mathfrak{s}} = \#A_1 \sum_{\mathfrak{s}|\mathfrak{r}} \prod_{\mathfrak{q}|\mathfrak{s}} (\mathrm{N}\mathfrak{q} - 2) = \#A_1 \prod_{\mathfrak{q}|\mathfrak{r}} (\mathrm{N}\mathfrak{q} - 1)$$

and the last is equal to $\#\mathrm{Gal}(K_n(\mathfrak{r})/K)$ since $G_{\mathfrak{r}} = \prod_{\mathfrak{q}|\mathfrak{r}} G_{\mathfrak{q}}$.

In order to prove that this set of generators form an independent set it is enough to prove that

$$\mathrm{rank}_{\mathbb{Z}} X_{n,\mathfrak{r}} \geq \#A \tag{5.2}$$

because we would obtain that the rank of the $\mathbb{Z}$-module is greater or equal than the size of a set of generators, which implies that the module is torsion free and the set of generators is a basis.

To prove it consider the following map

$$x_{n,\mathfrak{s}} \mapsto \prod_{\mathfrak{q}|\mathfrak{r}/\mathfrak{s}} N_{\mathfrak{q}} \prod_{\mathfrak{q}|\mathfrak{s}} \left((\mathrm{N}\mathfrak{q} - 1) + \left(\left(1 - \mathrm{Frob}_{\mathfrak{q}}^{-1}\right) + (\mathrm{N}\mathfrak{q} - 1) \right) \frac{N_{\mathfrak{q}}}{\mathrm{N}_{\mathfrak{q}} - 1} \right)$$

which send the indeterminate, $x_{n,\mathfrak{s}}$, to elements of $\mathbb{Q}[\mathrm{Gal}(K_n(\mathfrak{r})/K)]$. This can be extended $\mathbb{Z}[\mathrm{Gal}(K_n(\mathfrak{r})/K)]$-linearly to a map from $X_{n,\mathfrak{r}}$ to $\mathbb{Q}[\mathrm{Gal}(K_n(\mathfrak{r})/K)]$, since it respects the two relations of the module $X_{n,\mathfrak{r}}$. Indeed:

1. Let $\mathfrak{s} \mid \mathfrak{r}$. We need to see that if $\sigma \in \mathrm{Gal}(K_n(\mathfrak{r})/K_n(\mathfrak{s}))$, $\sigma x_{n,\mathfrak{s}}$ and $x_{n,\mathfrak{s}}$ have the same image. This follows from the fact that:

   $$\sigma = \prod_{\mathfrak{q}|\mathfrak{r}/\mathfrak{s}} \tau_{\mathfrak{q}}$$

   where $\tau_{\mathfrak{q}} \in \mathrm{Gal}(K_n(\mathfrak{r})/K_n(\mathfrak{r}/\mathfrak{q})$. Therefore:

   $$\sigma \prod_{\mathfrak{q}|\mathfrak{r}/\mathfrak{s}} N_{\mathfrak{q}} = \prod_{\mathfrak{q}|\mathfrak{r}/\mathfrak{s}} \tau_{\mathfrak{q}} N_{\mathfrak{q}} = \prod_{\mathfrak{q}|\mathfrak{r}/\mathfrak{s}} N_{\mathfrak{q}}.$$

2. Suppose that $\mathfrak{s}\bar{\mathfrak{q}} \mid \mathfrak{r}$. We should see that $N_{\bar{\mathfrak{q}}} x_{n,\mathfrak{s}\bar{\mathfrak{q}}}$ and $(1 - \mathrm{Frob}_{\bar{\mathfrak{q}}}^{-1}) x_{n,\mathfrak{s}}$ have the same image. This follows plainly from the fact that

   $$(\mathrm{N}\bar{\mathfrak{q}} - 1)\, N_{\bar{\mathfrak{q}}} = N_{\bar{\mathfrak{q}}} N_{\bar{\mathfrak{q}}}.$$

After these observations we therefore can define a $\mathbb{Q}$-linear map between the $\mathbb{Q}$-vector spaces $X_{n,\mathfrak{r}} \otimes \mathbb{Q}$ and $\mathbb{Q}[\mathrm{Gal}(K_n(\mathfrak{r})/K)]$

$$\varphi : X_{n,\mathfrak{r}} \otimes \mathbb{Q} \to \mathbb{Q}[\mathrm{Gal}(K_n(\mathfrak{r})/K)]$$

which is $\mathbb{Q}[\mathrm{Gal}(K_n(\mathfrak{r})/K)]$-equivariant by construction. Note that if we prove that φ is surjective, $\dim_{\mathbb{Q}} (X_{n,\mathfrak{r}} \otimes \mathbb{Q}) \geq \#\mathrm{Gal}(K_n(\mathfrak{r})/K)$ which shows (5.2) as we want.

To prove the surjectivity, let $\chi : \mathrm{Gal}(K_n(\mathfrak{r})/K) \to \mathbb{C}^\times$ a character of G with conductor $\mathfrak{s}$, i.e, $\mathfrak{s}$ is the largest ideal such that $\mathfrak{s} \mid \mathfrak{r}$ and $\mathrm{Gal}(K_n(\mathfrak{r})/K_n(\mathfrak{r}/\mathfrak{s})) \subset \ker \chi$. Then $\chi(\varphi(x_{n,\mathfrak{s}}) \neq 0$. Indeed

$$\prod_{\mathfrak{q}|\mathfrak{r}/\mathfrak{s}} \chi(N_\mathfrak{q}) = \prod_{\mathfrak{q}|\mathfrak{r}/\mathfrak{s}} (\mathrm{N}\mathfrak{q} - 1) \neq 0.$$

because for every $\mathfrak{q} \nmid \mathfrak{s}$ $\mathrm{Gal}(K_n(\mathfrak{r})/K_n(\mathfrak{r}/\mathfrak{q})) \subset \mathrm{Gal}(K_n(\mathfrak{r})/K_n(\mathfrak{s}))$. On the other hand, if $\mathfrak{q} \mid \mathfrak{s}$, the subgroup $\chi(G_\mathfrak{q}) \neq 1$. Using that $G_\mathfrak{q}$ is cyclic we get that $\chi(N_\mathfrak{q}) = 0$. Therefore

$$\chi\left(N_\mathfrak{q} \prod_{\mathfrak{q}|\mathfrak{s}} \left((\mathrm{N}\mathfrak{q} - 1) + \left(\left(1 - \mathrm{Frob}_\mathfrak{q}^{-1}\right) + (\mathrm{N}\mathfrak{q} - 1)\right) \frac{N_\mathfrak{q}}{\mathrm{N}_\mathfrak{q} - 1} \right)\right) = \prod_{\mathfrak{q}|\mathfrak{s}} (\mathrm{N}\mathfrak{q} - 1) \neq 0.$$

Combining these calculations yields

$$\chi(\varphi(x_{n,\mathfrak{s}})) = \prod_{\mathfrak{q}|\mathfrak{s}} (\mathrm{N}\mathfrak{q} - 1) \neq 0.$$

Now the result follows from the following lemma. □

Lemma 5.3.6. *Let G be an abelian group, X a $\mathbb{Q}[G]$-module and*

$$f : X \to \mathbb{Q}[G]$$

a $\mathbb{G}[Q]$-equivariant morphism. If for every character $\chi : G \to \mathbb{C}^\times$ the composition $\chi \circ f \neq 0$, then f is surjective.

Proof. The map f is a $\mathbb{Q}$-linear map. Therefore it is enough to prove that the induced map

$$f : X \otimes \mathbb{C} \to \mathbb{C}[G]$$

is surjective.

Recall, from representation theory of finite abelian groups, that multiplication by G induces a representation on $\mathbb{C}[G]$: the regular representation. Its decomposition in invariant subspaces is well known

$$\mathbb{C}[G] \cong \bigoplus_{i \in I} V_{\chi_i}$$

where $\{\chi_i\}_{i \in I}$ is the set of irreducible representations of G, which are all one dimensional, i.e. for every i there exists $v_i \in \mathbb{C}[G]$ generating V_{χ_i}.

For the sake of contradiction suppose that the map is not surjective. Since $\mathrm{im}f$ is a $\mathbb{C}[G]$-equivariant subspace it is plain to prove that

$$\mathrm{im}f = \bigoplus_{j \in J} V_{\chi_j}$$

for some subset $J \subset I$. Since $\mathrm{im}f \neq \mathbb{C}[G]$ there exists $i \in I \setminus J$. Now, from basic properties of orthogonality of characters it follows that $\chi_i(\mathrm{im}f) = 0$. Indeed, if $j \in J$ we have that for every $g \in G$

$$gv_j = \chi_j(g)v_j,$$

applying χ_i in both sides yields

$$(\chi_i(g) - \chi_j(g))\,\chi_i(v_j) = 0.$$

This must be true for every g, and since $\chi_i \neq \chi_j$ it has to be $\chi_i(v_j) = 0$. This is a contradiction with $\chi_i \circ f \neq 0$ and we are done. □

5.4 Kolyvagin's derivative

Consider an Euler system η, that we will identify with the universal Euler system. Fix M a power of a p and $n \geq 1$. We now explain how to construct a principal ideal of K_n starting from the unit $\eta(n, \mathfrak{r}) \in K_n(\mathfrak{r})$. This construction will be done only for $\mathfrak{r}$ in the following subgroup of $\mathcal{R}$.

Definition 5.4.1. Define $\mathcal{R}_{n,M}$ to be the subset of $\mathcal{R}$ with elements $\mathfrak{r} \in \mathcal{R}$ such that every prime $\mathfrak{q} \mid \mathfrak{r}$ satisfies:

- $\mathfrak{q}$ splits completely in K_n/K,
- $M \mid (\mathrm{N}\mathfrak{q} - 1)$.

In order to do the construction we will use the Kolyvagin's derivative operator. For every prime $\mathfrak{q} \in \mathcal{R}$ prime, fix $\sigma_\mathfrak{q} \in \mathrm{Gal}(K_n(\mathfrak{r})/K_n(\mathfrak{r}/\mathfrak{q}))$ a generator of the cyclic group.

Definition 5.4.2. If $\mathfrak{q} \in \mathcal{R}$ prime define

$$D_\mathfrak{q} = \sum_{i=1}^{\mathrm{N}\mathfrak{q}-2} i\sigma_\mathfrak{q}^i \in \mathbb{Z}[G_\mathfrak{q}].$$

For an arbitrary ideal $\mathfrak{r} \in \mathcal{R}$ define $D_\mathfrak{r} := \prod_{\mathfrak{q}|\mathfrak{r}} D_\mathfrak{q} \in \mathbb{Z}[G_\mathfrak{r}]$.

Remark 5.4.3. The definition of $D_{\mathfrak{q}}$ and $D_{\mathfrak{r}}$ depend on the choice of the generators $\sigma_{\mathfrak{q}}$. This is the reason we need to fix these generators.

By the way that $D_{\mathfrak{q}}$ is constructed it is clear that

Lemma 5.4.4. *If $\mathfrak{q} \in \mathcal{R}$ is a prime ideal and $\sigma_{\mathfrak{q}}$ is the fixed generator of $G_{\mathfrak{q}}$*

$$(\sigma_{\mathfrak{q}} - 1)D_{\mathfrak{q}} = (\mathrm{N}\mathfrak{q} - 1 - N_{\mathfrak{q}})$$

as elements of $\mathbb{Z}[G_{\mathfrak{q}}]$.

Proof. It is an easy calculation that uses that $G_{\mathfrak{q}}$ is cyclic of order $\mathrm{N}\mathfrak{q} - 1$

$$(\sigma_{\mathfrak{q}} - 1)D_{\mathfrak{q}} = (\sigma_{\mathfrak{q}} - 1)\sum_{i=1}^{\mathrm{N}\mathfrak{q}-2} i\sigma_{\mathfrak{q}}^i = \sum_{i=2}^{\mathrm{N}\mathfrak{q}-1}(i-1)\sigma_{\mathfrak{q}}^i - \sum_{i=1}^{\mathrm{N}\mathfrak{q}-2} i\sigma_{\mathfrak{q}}^i = (\mathrm{N}\mathfrak{q} - 1 - N_{\mathfrak{q}}).$$

□

Proposition 5.4.5. *If $\mathfrak{r} \in \mathcal{R}_{n,M}$ where $n \geq 1$, then $D_{\mathfrak{r}}x_{n,\mathfrak{r}} \in (X_{n,r}/MX_{n,\mathfrak{r}})^{G_{\mathfrak{r}}}$.*

Proof. We want to see that for every $\sigma \in G_{\mathfrak{r}}$

$$(\sigma - 1)D_{\mathfrak{r}}x_{n,\mathfrak{r}} \in MX_{n,\mathfrak{r}}.$$

The proof will be by induction on the number of primes dividing $\mathfrak{r}$. For the base case, suppose $\mathfrak{r} = \mathcal{O}$, then $G_{\mathfrak{r}} = 1$, the result is clear because $0x_{n,\mathfrak{r}} \in MX_{n,\mathfrak{r}}$. Now let $\mathfrak{r} \in \mathcal{R}_{n,M}$ and suppose that the result is proven by all ideals of $\mathcal{R}_{n,M}$ with less prime factors than $\mathfrak{r}$. Then for every $\mathfrak{q} \mid \mathfrak{r}$, denote $\mathfrak{s} = \mathfrak{r}\mathfrak{q}^{-1}$ and let $\sigma_{\mathfrak{q}}$ be the fixed generator of $G_{\mathfrak{q}} \subset G_{\mathfrak{r}}$. By Lemma 5.4.4:

$$(\sigma_{\mathfrak{q}} - 1)D_{\mathfrak{r}}x_{n,\mathfrak{r}} = (\sigma_{\mathfrak{q}} - 1)D_{\mathfrak{q}}D_{\mathfrak{s}}x_{n,\mathfrak{r}} = (\mathrm{N}\mathfrak{q} - 1 - N_{\mathfrak{q}})D_{\mathfrak{s}}x_{n,\mathfrak{r}}.$$

Since $M \mid (\mathrm{N}\mathfrak{q} - 1)$ is is clear that $(\mathrm{N}\mathfrak{q} - 1 - N_{\mathfrak{q}})D_{\mathfrak{s}}x_{n,\mathfrak{r}} \equiv -D_{\mathfrak{s}}N_{\mathfrak{q}}x_{n,\mathfrak{r}} \mod MX_{n,\mathfrak{r}}$. Now we use the distribution relation and the induction hypothesis on $\mathfrak{s}$

$$-D_{\mathfrak{s}}N_{\mathfrak{q}}x_{n,\mathfrak{r}} = (\mathrm{Frob}_{\mathfrak{q}}^{-1} - 1)x_{n,\mathfrak{s}} \equiv 0 \mod MX_{n,\mathfrak{r}}$$

To apply the induction hypothesis we have to ensure that $\mathrm{Frob}_{\mathfrak{q}} \in G_{\mathfrak{s}}$. This is true because $\mathfrak{q}$ splits completely in K_n/K so $\mathrm{Frob}_{\mathfrak{q}}$ fixes K_n. Since $\{\sigma_{\mathfrak{q}}\}_{\mathfrak{q}|\mathfrak{r}}$ for generate $G_{\mathfrak{r}}$ we are done. □

Now we have the tools to start the construction of the principal ideal.

Definition 5.4.6. Define a 1-cocycle $c \in H^1(G_{\mathfrak{r}}, K_n(\mathfrak{r})^\times)$

$$G_{\mathfrak{r}} \to K_n(\mathfrak{r})^\times, \quad c(\sigma) = \eta\left(\frac{(\sigma - 1)D_{\mathfrak{r}}x_{n,\mathfrak{r}}}{M}\right).$$

Remark 5.4.7. In the definition of $c(\sigma)$ we are using that $X_{n,\mathfrak{r}}$ is torsion free (Theorem 5.3.5) and therefore the element $(\sigma-1)D_{\mathfrak{r}}x_{n,\mathfrak{r}}/M$ is well defined, i.e. unique.

By Hilbert's Theorem 90 we have that $H^1(G_{\mathfrak{r}}, K_n(\mathfrak{r})) = 0$, hence there exists $\beta \in K_n(\mathfrak{r})^\times$ such that

$$c(\sigma) = \eta\left(\frac{(\sigma-1)D_{\mathfrak{r}}x_{n,\mathfrak{r}}}{M}\right) = \beta^{\sigma-1}.$$

Raising this equality to the M yields to

$$z = \frac{\eta(x_{n,\mathfrak{r}})^{D_{\mathfrak{r}}}}{\beta^M} \in K_n^\times.$$

The element β is well defined except for multiplication by an element of K_n. Hence, z is well defined in $K_n^\times/(K_n^\times)^M$.

Definition 5.4.8. With the same notation that used in the previous definition define

$$\kappa_{n,M}(\mathfrak{r}) = \frac{\eta(x_{n,\mathfrak{r}})^{D_{\mathfrak{r}}}}{\beta^M} \in K_n^\times/(K_n^\times)^M.$$

We will consider the principal ideals of F generated by elements of the form $\kappa_{n,M}(\mathfrak{r})$.

5.5 The Factorization Theorem

Unless stated otherwise, fix M a power of p, $n \geq 1$ and $\mathfrak{r} \in \mathcal{R}_{n,M}$. In order to simplify the notation denote $F = K_n$ and let $\mathcal{O}_F$ be its ring of integers. In this section we explain how to calculate the factorization of the ideal generated by $\kappa_{n,M}(\mathfrak{r}) \in F$ modulo Mth powers. The result will be in terms of $\kappa_{n,M}(\mathfrak{s})$ for ideals $\mathfrak{s} \mid \mathfrak{r}$. The reason why we need to consider the factorization modulo Mth powers is because $\kappa_{n,M}(\mathfrak{r})$ is only well defined in $F^\times/(F^\times)^M$.

We first introduce the notation that will be used to study these factorizations.

Definition 5.5.1. Denote the group of ideals of K_n additively as

$$\mathcal{I} = \bigoplus_{\mathfrak{Q}} \mathbb{Z}\mathfrak{Q},$$

where the sum is over all prime ideals $\mathfrak{Q}$ of F. If $\mathfrak{q}$ is a prime ideal of K, we define

$$\mathcal{I}_{\mathfrak{q}} = \bigoplus_{\mathfrak{Q}|\mathfrak{q}} \mathbb{Z}\mathfrak{Q}.$$

As we said we will study the factorizations of ideals modulo prime powers, hence we will work with $\mathcal{I}/M\mathcal{I}$ and $\mathcal{I}_{\mathfrak{q}}/M\mathcal{I}_{\mathfrak{q}}$.

For a given $y \in K_n$, denote by (y) the principal ideal generated by y, $(y)_{\mathfrak{q}}$ its projection on $\mathcal{I}_{\mathfrak{q}}$, $[y] \in \mathcal{I}/M\mathcal{I}$ the reduction modulo M and $[y]_{\mathfrak{q}}$ the respective projection.

Therefore, we are interested in

$$[\kappa_{n,M}(\mathfrak{r})] = \sum_{\mathfrak{q}} [\kappa_{n,M}(\mathfrak{r})]_{\mathfrak{q}}$$

where the sum is over the primes $\mathfrak{q}$ of K.

Lemma 5.5.2. *Let $\mathfrak{q}$ be a prime of K. For every $\mathfrak{Q} \mid \mathfrak{q}$ prime of F choose a prime $\bar{\mathfrak{Q}}$ of $F(\mathfrak{r})$ above it. Let e be the ramification index of $\mathfrak{Q}$ in the extension $F(\mathfrak{r})/F$ (by Corollary 5.2.3 e is equal for all $\mathfrak{Q}$). Choose a representative $z \in F^{\times}$ of $\kappa_{n,M}(\mathfrak{r})$*

$$z = \frac{\eta(x_{n,\mathfrak{r}})^{D_{\mathfrak{r}}}}{\beta^M}$$

with $\beta \in F(\mathfrak{r})$. Then

$$[\kappa_{n,M}(\mathfrak{r})]_{\mathfrak{q}} = \sum_{\mathfrak{Q}|\mathfrak{q}} \left(-\frac{M}{e} \mathrm{ord}_{\bar{\mathfrak{Q}}}(\beta) \mod M \right) \mathfrak{Q}.$$

Proof. By definition

$$[\kappa_{n,M}(\mathfrak{r})]_{\mathfrak{q}} = [z]_{\mathfrak{q}} = \sum_{\mathfrak{Q}|\mathfrak{q}} (\mathrm{ord}_{\mathfrak{Q}}(z) \mod M)\, \mathfrak{Q}.$$

and it is plain to see

$$\mathrm{ord}_{\mathfrak{Q}}(z) = \frac{1}{e}\mathrm{ord}_{\tilde{\mathfrak{Q}}}(z) = -\frac{M}{e}\mathrm{ord}_{\tilde{\mathfrak{Q}}}(\beta).$$

□

Remark 5.5.3. From this equality and Corollary 5.2.3 we see that if $\mathfrak{q}$ is a divisor of $\mathfrak{r}$, then $e = \mathrm{N}\mathfrak{q} - 1$, so $\mathrm{ord}_{\mathfrak{Q}}(z)$ is not necessarily a multiple of M. On the other hand, if $\mathfrak{q}$ is coprime to $\mathfrak{r}$, $e = 1$ so $[z]_{\mathfrak{q}} = 0$. This shows that even though the ideal generated by $\kappa_{n,M}(\mathfrak{r})$ in $F(\mathfrak{r})$ is trivial modulo Mth powers (since $\kappa_{n,M}(\mathfrak{r})$ equals to a unit divided by an Mth power) it is not necessarily trivial when considered as an ideal of F.

In order to have $[\kappa_{n,M}(\mathfrak{r})]_{\mathfrak{q}}$ we need to find $\mathrm{ord}_{\tilde{\mathfrak{Q}}}(\beta)$ for $\tilde{\mathfrak{Q}}$ above $\mathfrak{q}$ for the primes of K such that $\mathfrak{q} \mid \mathfrak{r}$.

Fix $\mathfrak{q} \in \mathcal{R}_{n,M}$ a prime of K. We will construct a function, $\phi_{\mathfrak{q}}$ that, by the end of this section, will allow us to relate $\mathrm{ord}_{\tilde{\mathfrak{Q}}}(\beta)$ with the element $\kappa_{n,M}(\mathfrak{r}\mathfrak{q}^{-1})$. We start by defining a map

$$\phi'_{\mathfrak{q}} : (\mathcal{O}_F/\mathfrak{q}\mathcal{O}_F)^{\times} \to \mathcal{I}_{\mathfrak{q}}/M\mathcal{I}_{\mathfrak{q}}$$

that after a small modification will become our desired map. Notice that $\mathfrak{q}$ splits completely in F

$$(\mathcal{O}_F/\mathfrak{q}\mathcal{O}_F)^{\times} \cong \prod_{\mathfrak{Q}|\mathfrak{q}} (\mathcal{O}_F/\mathfrak{Q})^{\times}$$

and every of this terms is cyclic of order $\mathrm{N}\mathfrak{q} - 1$. On the other hand

$$\mathcal{I}_{\mathfrak{q}}/M\mathcal{I}_{\mathfrak{q}} \cong \oplus_{\mathfrak{Q}|\mathfrak{q}}(\mathbb{Z}/M\mathbb{Z}).$$

Since $M \mid (\mathrm{N}\mathfrak{q}-1)$, to define $\phi'_{\mathfrak{q}}$ is to choose a generator of the cyclic group $(\mathcal{O}_F/\mathfrak{Q})^{\times}$ for every $\mathfrak{Q} \mid \mathfrak{q}$ and map it to $1 \in \mathbb{Z}/M\mathbb{Z}$.

Now we explain how we choose these generators. For $\mathfrak{Q}$ dividing $\mathfrak{q}$ choose a prime $\mathfrak{Q}'$ of $F(\mathfrak{q})$ above it and consider $\pi_{\mathfrak{Q}}$ a local parameter at the prime $\mathfrak{Q}'$. Since the local field extension $F(\mathfrak{q})_{\mathfrak{Q}'}/F_{\mathfrak{Q}}$ is totally tamely ramified we have that the map

$$\mathrm{Gal}(F(\mathfrak{q})/F) \to {\mathcal{O}_{F(\mathfrak{q}),\mathfrak{Q}'}}^{\times} \to (\mathcal{O}_F/\mathfrak{Q})^{\times}, \quad \sigma \mapsto \pi_{\mathfrak{Q}}^{(1-\sigma)} \mapsto [\pi_{\mathfrak{Q}}^{(1-\sigma)}] \tag{5.3}$$

is a group isomorphism ([Ser13], Chapter IV Proposition 5).

Definition 5.5.4. For $\mathfrak{Q}$ as above, define $\gamma_{\mathfrak{Q}} \in (\mathcal{O}_F/\mathfrak{Q})^{\times}$ to be the image of the fixed generator $\sigma_{\mathfrak{q}} \in G_{\mathfrak{q}}$ (see Remark 5.4.3) by the map in (5.3). It is a generator of $(\mathcal{O}_F/\mathfrak{Q})^{\times}$.

Definition 5.5.5. Define the map

$$\phi'_{\mathfrak{q}} : (\mathcal{O}_F/\mathfrak{q})^{\times} \to \mathcal{I}_{\mathfrak{q}}/M\mathcal{I}_{\mathfrak{q}}$$

as follows: given $\alpha \in (\mathcal{O}_F/\mathfrak{q})^{\times}$ define, for every $\mathfrak{Q} \mid \mathfrak{q}$, $a_{\mathfrak{Q}}(\alpha) \in \mathbb{Z}$ such that $\alpha \equiv \gamma_{\mathfrak{Q}}^{a_{\mathfrak{Q}}(\alpha)}$ mod $\mathfrak{Q}$. Then define

$$\phi'_{\mathfrak{q}}(\alpha) = \sum_{\mathfrak{Q}|\mathfrak{q}} (a_{\mathfrak{Q}}(\alpha) \mod M)\, \mathfrak{Q}.$$

It is clear that

Proposition 5.5.6. *The map $\phi'_{\mathfrak{q}}$ is surjective,* $\mathrm{Gal}(F/K)$*-equivariant and its kernel is precisely the set of Mth powers of $(\mathcal{O}_F/\mathfrak{q})^{\times}$.*

Definition 5.5.7. We have a well defined map

$$j_{\mathfrak{q}} : \left\{ \kappa \in F^\times / \left(F^\times\right)^M : [\kappa]_{\mathfrak{q}} = 0 \right\} \to \left(\mathcal{O}_F/\mathfrak{q}\right)^\times / \left(\left(\mathcal{O}_F/\mathfrak{q}\right)^\times\right)^M$$

where for every $\kappa \in F^\times/\left(F^\times\right)^M$ we choose a representative $z \in \mathcal{O}_F^\times$ such that $\mathrm{ord}_{\mathfrak{Q}}(z) = 0$ for every $\mathfrak{Q} \mid \mathfrak{q}$. Define $\phi_{\mathfrak{q}} = \phi'_{\mathfrak{q}} \circ j_{\mathfrak{q}}$.

Before stating and proving the Factorization Theorem, we prove the following lemma that will be necessary.

Lemma 5.5.8. *Let η be an Euler System and $\mathfrak{q} \in \mathcal{R}$ prime. Write $\mathrm{N}\mathfrak{q} - 1 = dp^k$ with $(d,p) = 1$. Then, for every $n \geq 1$ and $\mathfrak{r} \in \mathcal{R}$ coprime to $\mathfrak{q}$*

$$\eta(n, \mathfrak{q}\mathfrak{r})^d \equiv \eta(n, \mathfrak{r})^{d\mathrm{Frob}_{\mathfrak{q}}^{-1}}$$

modulo every prime above $\mathfrak{q}$.

Proof. Let $m \geq n$ and $G = \mathrm{Gal}(K_m(\mathfrak{q}\mathfrak{r})/K_n(\mathfrak{q}\mathfrak{r}))$. Let H be the decomposition group of G at a prime $\tilde{\mathfrak{Q}}$ of $K_m(\mathfrak{q}\mathfrak{r})$ above $\mathfrak{q}$. Denote by H' a set of representatives of G/H and

$$N_H = \sum_{\sigma \in H} \sigma, \quad N_{H'} = \sum_{\sigma \in H'} \sigma.$$

Recall the norm compatibility relations of the definition of an Euler system, we will start working with

$$\mathrm{N}_{K_m(\mathfrak{r}\mathfrak{q})/K_m(\mathfrak{r})} \eta(m, \mathfrak{r}\mathfrak{q}) = \eta(m, \mathfrak{r})^{1-\mathrm{Frob}_{\mathfrak{q}}^{-1}},$$

Since the primes above $\mathfrak{q}$ are totally ramified in $K_m(\mathfrak{q}\mathfrak{r})/K_m(\mathfrak{r})$ (Theorem 2.6.4 (5)), all the elements of $\mathrm{Gal}(K_m(\mathfrak{q}\mathfrak{r})/K_m(\mathfrak{r}))$ reduce to the identity modulo $\tilde{\mathfrak{Q}}$. Hence

$$\mathrm{N}_{K_m(\mathfrak{r}\mathfrak{q})/K_m(\mathfrak{r})} \eta(m, \mathfrak{r}\mathfrak{q}) \equiv \eta(m, \mathfrak{r}\mathfrak{q})^{\mathrm{N}\mathfrak{q}-1} \mod \tilde{\mathfrak{Q}}.$$

On the other hand, using the characterization of $\mathrm{Frob}_{\mathfrak{q}}$ it is easy to see that

$$\eta(m, \mathfrak{r})^{(1-\mathrm{Frob}_{\mathfrak{q}}^{-1})} \equiv \left(\eta(m, \mathfrak{r})^{\mathrm{Frob}_{\mathfrak{q}}}\right)^{\mathrm{N}\mathfrak{q}-1} \mod \tilde{\mathfrak{Q}}.$$

So, the first equation becomes

$$\eta(m, \mathfrak{r}\mathfrak{q})^{\mathrm{N}\mathfrak{q}-1} \equiv \left(\eta(m, \mathfrak{r})^{\mathrm{Frob}_{\mathfrak{q}}^{-1}}\right)^{\mathrm{N}\mathfrak{q}-1} \mod \tilde{\mathfrak{Q}}. \tag{5.4}$$

The second norm compatibility relation implies

$$\mathrm{N}_{K_m(\mathfrak{q}\mathfrak{r})/K_n(\mathfrak{q}\mathfrak{r})} \eta(m, \mathfrak{q}\mathfrak{r}) = \eta(n, \mathfrak{q}\mathfrak{r}).$$

Note that

$$\mathrm{N}_{K_m(\mathfrak{q}\mathfrak{r})/K_n(\mathfrak{q}\mathfrak{r})}\eta(m,\mathfrak{q}\mathfrak{r}) = \eta(m,\mathfrak{q}\mathfrak{r})^{N_H N_{H'}}.$$

But it is easy to know how N_H acts on the elements of the residue field, because the automorphisms of a finite field are generated by the Frobenius automorphism, i.e.

$$\eta(m,\mathfrak{q}\mathfrak{r})^{N_H} \equiv \eta(m,\mathfrak{q}\mathfrak{r})^t$$

where, if we call h the residual degree at $\mathfrak{q}$ of the extension $K_n(\mathfrak{q}\mathfrak{r})/K$

$$t = \sum_{i=0}^{\#H-1} (\mathrm{N}\mathfrak{q})^{hi} \equiv \#H \mod (\mathrm{N}\mathfrak{q}-1)$$

Hence, the second compatibility relation becomes

$$\eta(m,\mathfrak{q}\mathfrak{r})^{tN_{H'}} \equiv \eta(n,\mathfrak{q}\mathfrak{r}) \mod \tilde{\mathfrak{Q}} \tag{5.5}$$

Now, we observe that the cardinality of G is a power of p and hence so is the cardinality of H. Moreover, $\mathrm{Gal}(K_m(\mathfrak{q}\mathfrak{r})/K_n(\mathfrak{q}\mathfrak{r}))$ is unramified at $\mathfrak{q}$ for all $m \geq n$, so for every value of m we obtain distinct finite extensions of the residue field of $K_n(\mathfrak{q}\mathfrak{r})$. This means that the decomposition group H can be arbitrarily large. So choose m such that $p^k \mid (\#H)$ and write $t = p^k t'$.

Now we can combine (5.5) and (5.4) to say that modulo $\tilde{\mathfrak{Q}}$

$$\eta(n,\mathfrak{q}\mathfrak{r})^d \equiv \eta(m,\mathfrak{q}\mathfrak{r})^{N_{H'}dt} \equiv \left(\eta(m,\mathfrak{q}\mathfrak{r})^{N_{H'}}\right)^{(\mathrm{N}\mathfrak{q}-1)t'} \equiv \left(\eta(m,\mathfrak{r})^{\mathrm{Frob}_{\mathfrak{q}}^{-1}}\right)^{(\mathrm{N}\mathfrak{q}-1)N_{H'}t'}.$$

Where for the last congruence we applied (5.4) to $(\eta_{m,\mathfrak{q}\mathfrak{r}})^{N_{H'}}$ since it is plain to see that the proof is analogous. Now, from Theorem 2.6.4 it is easy to see that the restriction map $\mathrm{Gal}(K_m(\mathfrak{q}\mathfrak{r})/K_n(\mathfrak{q}\mathfrak{r})) \to \mathrm{Gal}(K_m(\mathfrak{r})/K_n(\mathfrak{r}))$ and from here it follows that we can apply (5.5) to say

$$\left(\eta(m,\mathfrak{r})^{\mathrm{Frob}_{\mathfrak{q}}^{-1}}\right)^{(\mathrm{N}\mathfrak{q}-1)N_{H'}t'} = \left(\eta(m,\mathfrak{r})^{tN_{H'}}\right)^{d\mathrm{Frob}_{\mathfrak{q}}^{-1}} \equiv \eta(m,\mathfrak{r})^{d\mathrm{Frob}_{\mathfrak{q}}^{-1}} \mod \tilde{\mathfrak{Q}}$$

and we are done.

□

Theorem 5.5.9 (Factorization Theorem)**.** *Consider $\kappa_{n,M}(\mathfrak{r})$ and $\mathfrak{q}$ a prime ideal of K. Then:*

1. *If $\mathfrak{q} \nmid \mathfrak{r}$, $[\kappa_{n,M}(\mathfrak{r})]_{\mathfrak{q}} = 0$,*
2. *If $\mathfrak{q} \mid \mathfrak{r}$: $[\kappa_{n,M}(\mathfrak{r})]_{\mathfrak{q}} = \phi_{\mathfrak{q}}(\kappa_{n,M}(\mathfrak{r}\mathfrak{q}^{-1}))$.*

Proof. Let $z_{\mathfrak{r}}$ be a representative of $\kappa_{n,M}(\mathfrak{r})$, i.e.

$$z_{\mathfrak{r}} = \frac{\eta(x_{n,M})^{D_{\mathfrak{r}}}}{\beta_{\mathfrak{r}}^{M}} \in F^{\times}.$$

Then, we have to find $[z]_{\mathfrak{q}}$, and as it is done in Lemma 5.5.2

$$[z_{\mathfrak{r}}]_{\mathfrak{q}} = \sum_{\mathfrak{Q}|\mathfrak{q}} (\mathrm{ord}_{\mathfrak{Q}}(z) \mod M)\,\mathfrak{Q}$$

where

$$\mathrm{ord}_{\mathfrak{Q}}(z_{\mathfrak{r}}) = \frac{1}{e}\mathrm{ord}_{\tilde{\mathfrak{Q}}}(z_{\mathfrak{r}}) = -\frac{M}{e}\mathrm{ord}_{\tilde{\mathfrak{Q}}}(\beta_{\mathfrak{r}}).$$

where we choose $\mathfrak{Q}$ a prime of F above $\mathfrak{q}$ and $\tilde{\mathfrak{Q}}$ a prime of $F(\mathfrak{r})$ above $\mathfrak{q}$.

1. If $\mathfrak{q} \nmid \mathfrak{r}$, then $\mathfrak{q}$ is unramified at $F(\mathfrak{r})$, this implies that $e = 1$ and hence $[z]_{\mathfrak{q}} = 0$ proving the first statement.

2. Suppose that $\mathfrak{q} \mid \mathfrak{r}$ and let $\mathfrak{s} = \mathfrak{r}\mathfrak{q}^{-1}$. Then we have the extensions $F(\mathfrak{r})/F(\mathfrak{q})/F$.

   Let $\mathfrak{Q}'$ the prime of $F(\mathfrak{q})$ above $\mathfrak{Q}$ (recall that $F(\mathfrak{q})/F$ is totally ramified at $\mathfrak{Q}$) and let $\tilde{\mathfrak{Q}}$ be a prime of $F(\mathfrak{r})$ above $\mathfrak{Q}'$ (also recall that the extension $F(\mathfrak{r})/F(\mathfrak{q})$ is unramified at $\mathfrak{Q}'$). In this case the ramification index is $e = \mathrm{N}\mathfrak{q} - 1$ hence

   $$\mathrm{ord}_{\mathfrak{Q}}(z) = \frac{M}{1 - \mathrm{N}\mathfrak{q}}\mathrm{ord}_{\tilde{\mathfrak{Q}}}(\beta).$$

   Call $c_{\mathfrak{Q}} = \mathrm{ord}_{\tilde{\mathfrak{Q}}}(\beta)$, and let $\pi_{\mathfrak{Q}}$ be a local parameter of $F(\mathfrak{q})$ at $\mathfrak{Q}'$. Then $\pi_{\mathfrak{Q}}$ is also a local parameter of $F(\mathfrak{r})$ at $\tilde{\mathfrak{Q}}$ because the extension $F(\mathfrak{r})/F(\mathfrak{q})$ is uramified at $\mathfrak{Q}'$. This means that we can write

   $$\beta_{\mathfrak{r}} = \pi_{\mathfrak{Q}}^{c_{\mathfrak{Q}}}\alpha_{\mathfrak{Q}}$$

   where $\alpha_{\mathfrak{Q}}$ is a unit in the completion of $F(\mathfrak{r})$ at the prime $\tilde{\mathfrak{Q}}$.

   Now we consider $\sigma_{\mathfrak{q}}$ the generator of $G_{\mathfrak{q}} = \mathrm{Gal}(F(\mathfrak{q})/F)$. As it is said in Corollary 5.2.4, $G_{\mathfrak{q}}$ can be identified with $\mathrm{Gal}(F(\mathfrak{r})/F(\mathfrak{s}))$ and it is easy to see that it corresponds to the inertia subgroup at $\mathfrak{Q}'$ of $\mathrm{Gal}(F(\mathfrak{r})/F)$. Therefore, since $\alpha_{\mathfrak{Q}}$ is a unit

   $$\beta_{\mathfrak{r}}^{1-\sigma_{\mathfrak{q}}} = \left(\pi_{\mathfrak{Q}}^{1-\sigma_{\mathfrak{q}}}\right)^{c_{\mathfrak{Q}}} (\alpha_{\mathfrak{Q}})^{1-\sigma_{\mathfrak{q}}} \equiv \left(\pi_{\mathfrak{Q}}^{1-\sigma_{\mathfrak{q}}}\right)^{c_{\mathfrak{Q}}} \equiv \gamma_{\mathfrak{Q}}^{c_{\mathfrak{Q}}} \mod \tilde{\mathfrak{Q}} \tag{5.6}$$

   where we used the expression of the generator $\gamma_{\mathfrak{Q}}$ (see Definition 5.5.5).

Now we proceed to calculate $\phi_{\mathfrak{q}}(\kappa_{n,M}(\mathfrak{s}))$. For this let

$$z_{\mathfrak{s}} = \frac{\eta(x_{n,M})^{D_{\mathfrak{s}}}}{\beta_{\mathfrak{s}}^{M}} \in \mathcal{O}_F^{\times}$$

be an integral representative of $\kappa_{n,M}(\mathfrak{s})$. Therefore, following Definition 5.5.7, to compute $\phi_{\mathfrak{q}}(\kappa_{n,M}(\mathfrak{s}))$ we need to find $z_{\mathfrak{s}} \mod \mathfrak{Q}$ for every $\mathfrak{Q} \mid \mathfrak{q}$. In order to do so write $\mathrm{N}\mathfrak{q} - 1 = dp^k$ where $(d,p) = 1$ and we will compute $\beta_{\mathfrak{r}}^{d(\sigma_{\mathfrak{q}}-1)}$ modulo $\tilde{\mathfrak{Q}}$ in terms of $z_{\mathfrak{s}} \mod \tilde{\mathfrak{Q}}$

$$\beta_{\mathfrak{r}}^{d(\sigma_{\mathfrak{q}}-1)} = \eta\left(\frac{(\sigma_{\mathfrak{q}}-1)D_{\mathfrak{r}}x_{n,\mathfrak{r}}}{M}\right)^d = \eta\left(\frac{(\mathrm{N}\mathfrak{q}-1-N_{\mathfrak{q}})D_{\mathfrak{s}}x_{n,\mathfrak{r}}}{M}\right)^d =$$
$$= \left(\eta(x_{n,\mathfrak{r}})^d\right)^{D_{\mathfrak{s}}\frac{\mathrm{N}\mathfrak{q}-1}{M}} \eta\left(\frac{(1-\mathrm{Frob}_{\mathfrak{q}}^{-1})x_{n,\mathfrak{s}}}{M}\right)^d$$

where we used Lemma 5.4.4 and then the distribution relation satisfied by the Euler System (Definition 5.3.2). Now applying Lemma 5.5.8 at the first term of the product and the definition of $\beta_{\mathfrak{s}}$ at the second one we can write

$$\left(\eta(x_{n,\mathfrak{r}})^d\right)^{D_{\mathfrak{s}}\frac{\mathrm{N}\mathfrak{q}-1}{M}} \eta\left(\frac{(1-\mathrm{Frob}_{\mathfrak{q}}^{-1})x_{n,\mathfrak{s}}}{M}\right)^d \equiv \eta(x_{n,\mathfrak{s}})^{d\mathrm{Frob}_{\mathfrak{q}}^{-1}D_{\mathfrak{s}}\left(\frac{\mathrm{N}\mathfrak{q}-1}{M}\right)}\beta_{\mathfrak{s}}^{d(\mathrm{Frob}_{\mathfrak{q}}{}^{-1}-1)} \mod \tilde{\mathfrak{Q}}.$$

But note that since $\mathfrak{q}$ splits in F, $\mathrm{Frob}_{\mathfrak{q}}$ fixes F, therefore

$$\left(\frac{\eta(D_{\mathfrak{s}}x_{n,\mathfrak{s}})}{\beta_{\mathfrak{s}}^{M}}\right)^{\mathrm{Frob}_{\mathfrak{q}}^{-1}} = \frac{\eta(D_{\mathfrak{s}}x_{n,\mathfrak{s}})}{\beta_{\mathfrak{s}}^{M}} = z_{\mathfrak{s}}.$$

Hence, we have that modulo $\tilde{\mathfrak{Q}}$

$$\eta(x_{n,\mathfrak{s}})^{d\mathrm{Frob}_{\mathfrak{q}}^{-1}D_{\mathfrak{s}}\left(\frac{\mathrm{N}\mathfrak{q}-1}{M}\right)}\beta_{\mathfrak{s}}^{d(\mathrm{Frob}_{\mathfrak{q}}{}^{-1}-1)} \equiv z_{\mathfrak{s}}^{d\frac{\mathrm{N}\mathfrak{q}-1}{M}}\beta_{\mathfrak{s}}^{(\mathrm{Frob}_{\mathfrak{q}}^{-1})d(\mathrm{N}\mathfrak{q}-1)}\beta_{\mathfrak{s}}^{d(\mathrm{Frob}_{\mathfrak{q}}^{-1}-1)}$$

Finally, use the characterization of $\mathrm{Frob}_{\mathfrak{q}}^{-1}$ to note that

$$\beta_{\mathfrak{s}}^{(\mathrm{Frob}_{\mathfrak{q}}^{-1})d(\mathrm{N}\mathfrak{q}-1)}\beta_{\mathfrak{s}}^{d(\mathrm{Frob}_{\mathfrak{q}}^{-1}-1)} = \frac{\left(\beta_{\mathfrak{s}}^{d}\right)^{(\mathrm{Frob}_{\mathfrak{q}}^{-1})(\mathrm{N}\mathfrak{q})}}{\beta_{\mathfrak{s}}^{d}} \equiv 1 \mod \tilde{\mathfrak{Q}}$$

so we can conclude

$$\beta_{\mathfrak{r}}^{d(\sigma_{\mathfrak{q}}-1)} \equiv z_{\mathfrak{s}}^{d\frac{\mathrm{N}\mathfrak{q}-1}{M}} \mod \tilde{\mathfrak{Q}}$$

but using (5.6) we get

$$z_{\mathfrak{s}}^{d\frac{1-\mathrm{N}\mathfrak{q}}{M}} \equiv \gamma_{\mathfrak{Q}}^{dc_{\mathfrak{Q}}} \mod \tilde{\mathfrak{Q}}.$$

From this expression and the fact that $(d,p)=1$, and therefore $(d,M)=1$ it is plain to obtain the desired result

$$\phi_{\mathfrak{q}}(z_{\mathfrak{s}}) = \frac{M}{1-\mathrm{N}\mathfrak{q}} \sum_{\mathfrak{Q}|\mathfrak{q}} c_{\mathfrak{Q}}\mathfrak{Q} = \frac{M}{1-\mathrm{N}\mathfrak{q}} \sum_{\mathfrak{Q}|\mathfrak{q}} \frac{-(\mathrm{N}\mathfrak{q}-1)}{M} \mathrm{ord}_{\mathfrak{Q}}(z_{\mathfrak{r}})\mathfrak{Q} = [z_{\mathfrak{r}}]_{\mathfrak{q}}$$

□

Chapter 6

Bounding the ideal class group

Let K be an imaginary quadratic field of class nubmer 1. Denote by $\mathcal{O}$ its ring of integers. Let E be an elliptic curve defined over K with complex multiplication by $\mathcal{O}$ and denote by $\mathfrak{f}$ the conductor of its associated Hecke character ψ. Fix an ideal $\mathfrak{a}$ of K prime to $6\mathfrak{f}$ and a prime ideal $\mathfrak{p}$ of K coprime to $6\mathfrak{f}\mathfrak{a}$ above a rational prime p which splits in K. We will denote by $F = K(E[\mathfrak{p}])$, $\Delta = \mathrm{Gal}(F/K)$ and A the ideal class group of F. Let $\mathcal{O}_F$ be the ring of integers of F and μ_F the set of roots of unity in F. Finally, fix M a power of p, denote by μ_M the set of Mth roots of unity and let $F_M = F(\mu_M)$.

The goal of this chapter is to use elliptic units to bound A^χ where χ is the character of an irreducible representation of Δ (see Definition 3.5.4 for the definition of A^χ). The Factorization Theorem proved in the previous chapter is the result that we will need. We are going to found this bound only for the case where p splits in K. It is not difficult to generalize the result for any rational prime but we do not need it for this proof. For this reason we decided to focus on the simplest case.

We follow closely the proof presented in [Rub99] Chapter 9. There, the result is proven for any rational prime p.

6.1 An application of the Chebotarev Theorem

Definition 6.1.1. There is a natural map

$$\mathrm{Hom}(A, \mathbb{Z}/M\mathbb{Z}) \to \mathrm{Hom}(G_F, \mathbb{Z}/M\mathbb{Z})$$

such that for a given $\alpha \in \mathrm{Hom}(A, \mathbb{Z}/M\mathbb{Z})$ we can define an element of $\mathrm{Hom}(G_F, \mathbb{Z}/M\mathbb{Z})$, that will be denoted also by α via the compositions

$$G_F \to \mathrm{Gal}(H/F) \xrightarrow{\sim} A \xrightarrow{\alpha} \mathbb{Z}/M\mathbb{Z}$$

where H is the Hilbert Class Field of F.

We will use this two notions of α interchangeably.

Lemma 6.1.2. *The map*

$$\mathrm{Hom}(A, \mathbb{Z}/M\mathbb{Z}) \to \mathrm{Hom}(G_F, \mathbb{Z}/M\mathbb{Z}) \to \mathrm{Hom}(G_{F_M}, \mathbb{Z}/M\mathbb{Z})$$

is injective.

Proof. Let $\alpha \in \mathrm{Hom}(A, \mathbb{Z}/M\mathbb{Z})$ and consider the corresponding $\alpha \in \mathrm{Hom}(G_F, \mathbb{Z}/M\mathbb{Z})$. It is easy to see that $\ker(\alpha)$ is a finite index open subgroup of G_F and that $G_F/\ker(\alpha)$ is isomorphic to a subgroup of $\mathbb{Z}/M\mathbb{Z}$. Hence, there exists a finite p-extension L/F such that $\mathrm{Gal}(\bar{F}/L) \cong \ker(\alpha)$. Moreover, since α factors through the quotient $\mathrm{Gal}(H/F)$, $L \subset H$.

Now suppose that α is zero in G_{F_M}. This implies that $L \subset F_M$. On the other hand, we already saw that $L \subset H$, which means that L is unramified at all primes. However, the p-part of $\mathrm{Gal}(F_M/F)$ is totally ramified at p. This implies that $L = F$ so $\alpha = 0$ in G_F. □

Lemma 6.1.3. *The natural map*

$$F^\times / \left(F^\times\right)^M \to F_M^\times / \left(F_M^\times\right)^M$$

is injective.

Proof. The kummer map gives the isomorphisms

$$F^\times / \left(F^\times\right)^M \xrightarrow{\sim} H^1(F, \mu_M), \quad F_M^\times / \left(F_M^\times\right)^M \xrightarrow{\sim} H^1(F_M, \mu_M).$$

Hence the map of the lemma can be rewritten as the restriction map

$$H^1(F, \mu_M) \to H^1(F_M, \mu_M).$$

Its kernel is given by the inflation restriction exact sequence and since $\mu_M \subset F_M$ it is precisely $H^1(F_M/F, \mu_M)$. Notice that, by choosing a generator of $\mu_M \cong \mathbb{Z}/p^n\mathbb{Z}$, we can view $\mathrm{Gal}(F_M/F)$ as subgroup of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ which acts on μ_M by multiplication. The result follows from the following lemma. □

Lemma 6.1.4. *Let $C \subset (\mathbb{Z}/p^n\mathbb{Z})^\times$ acting on $\mathbb{Z}/p^n\mathbb{Z}$ via multiplication. Then*

$$H^1(C, \mathbb{Z}/p^n\mathbb{Z}) = 0.$$

Proof. Notice that C is cyclic, choose $g \in C$ a generator and let m be its order. Let $0 \leq r \leq n$ such that $g \equiv 1 \mod p^r$ but $g \not\equiv 1 \mod p^{r+1}$.

It is plain to prove that the group of coboundaries $B^1(C, \mathbb{Z}/p^n\mathbb{Z})$ has precisely p^{n-r} elements. To conclude the proof it is enough to see that $Z^1(C, \mathbb{Z}/p^n\mathbb{Z})$, the group of cocycles has the same number of elements.

Note that $c \in Z^1(C, \mathbb{Z}/p^n\mathbb{Z})$ is completely determined by $c(g)$, since the cocycle condition implies that

$$c(g^k) = (1 + g + \cdots + g^{k-1})c(g). \tag{6.1}$$

In addition, the condition $c(g^m) = c(1) = 0$ implies that

$$(1 + g + \cdots + g^{m-1})c(g) = 0$$

in $\mathbb{Z}/p^n\mathbb{Z}$. This forces $c(g) \equiv 0 \mod p^r$.

It is straightforward to prove that any map $c : C \to \mathbb{Z}/p^n\mathbb{Z}$ such that $c(g) \equiv 0 \mod p^r$ defined by (6.1) is a cocycle. Hence $\#Z^1(C, \mathbb{Z}/p^n\mathbb{Z}) = p^{n-r}$ and we are done. □

The next proposition, where we will apply the Chebotarev density theorem, is essential for the argument that we will do in order to bound the size of A^χ.

Proposition 6.1.5. *Let $\alpha \in \mathrm{Hom}(A, \mathbb{Z}/M\mathbb{Z})$ nonzero and $\kappa \in F^\times/(F^\times)^M$. Then, there exists a prime $\mathfrak{q} \in \mathcal{R}_{1,M}$ of K and a prime $\mathfrak{Q}$ of F above $\mathfrak{q}$ such that:*

1. *$\alpha(\mathfrak{c}) \neq 0$, where $\mathfrak{c}$ is the class of $\mathfrak{Q}$ in A,*
2. *$[\kappa]_\mathfrak{q} = 0$ and $d\phi_\mathfrak{q}(\kappa) = 0$ if and only if $\kappa^d \in (F^\times)^M$ for every $d \in \mathbb{Z}$.*

Proof. Let t be the order of κ in $F^\times/(F^\times)^M$. Define $\rho \in \mathrm{Hom}(G_{F_M}, \mu_M)$ as

$$\rho : G_{F_M} \to \mu_M, \quad \sigma \mapsto \left(\kappa^{1/M}\right)^{\sigma - 1}. \tag{6.2}$$

Define

$$H_\alpha = \{\sigma \in G_{F_M} : \alpha(\sigma) = 0\},$$
$$H_\rho = \{\sigma \in G_{F_M} : \rho(\sigma) \text{ has order less than } t\}.$$

By Lemma 6.1.2, $H_\alpha \neq G_{F_M}$. Similarly, $H_\rho \neq G_{F_M}$. Otherwise, there would be $s < t$ such that $\rho(\sigma)^s = 1$ for all $\sigma \in G_{F_M}$. From the definition of ρ in (6.2) we get that κ has order $s < t$ in $F_M^\times/\left(F_M^\times\right)^M$ which is a contradiction with the injectivity of Lemma 6.1.3. Therefore, since a group can not be the union of two proper subgroups we can choose $\gamma \in G_{F_M}$ such that $\gamma \notin H_\rho \cup H_\alpha$.

Let L be a finite Galois extension of F containing F_M, H (the Hilbert class field of F) and such that both α and ρ are trivial in the subgroup G_L. By the Chebotarev density theorem we can choose, a prime $\mathfrak{Q}'$ of L coprime to $6\mathfrak{p}\mathfrak{a}\mathfrak{f}$ such that, if $\mathfrak{q}$ is the prime of K below $\mathfrak{Q}'$, $[\kappa]_{\mathfrak{q}} = 0$ and

$$\gamma|_L = \mathrm{Frob}_{\mathfrak{Q}'}.$$

Let $\mathfrak{Q}$ be the prime of F below $\mathfrak{Q}'$ and $\mathfrak{c}$ the ideal class of $\mathfrak{Q}$ in A. Since, $\mathrm{Frob}_{\mathfrak{Q}'}|_H = \mathrm{Frob}_{\mathfrak{Q}}$, using the identifications of α in Definition 6.1.1

$$\alpha(\mathfrak{c}) = \alpha(\mathrm{Frob}_{\mathfrak{Q}}) = \alpha(\gamma) \neq 0.$$

Moreover, since γ fixes F_M, $\mathrm{Frob}_{\mathfrak{Q}}$ fixes F_M which implies that $\mathfrak{Q} \in \mathcal{R}_{1,M}$. This proves (1).

For the second condition note that $\kappa^{1/M} \in L$ because ρ is trivial in G_L. Therefore

$$\left(\kappa^{1/M}\right)^{\gamma-1} = \left(\kappa^{1/M}\right)^{\mathrm{Frob}_{\mathfrak{Q}'}-1}.$$

And using that $\gamma \notin H_\rho$, $\left(\kappa^{1/M}\right)^{\mathrm{Frob}_{\mathfrak{Q}'}-1}$ is a root of unity of order t. It is plain to prove that it reduces to an element of order t in $(\mathcal{O}_L/\mathfrak{Q}')^\times$, in other words, $\left(\kappa^{1/M}\right)^{\mathrm{N}\mathfrak{q}-1}$ has order t in $(\mathcal{O}_L/\mathfrak{Q}')^\times$. Therefore κ has order $(\mathrm{N}\mathfrak{q}-1)M/t$ in $(\mathcal{O}_F/\mathfrak{Q})^\times$ which implies that κ has order t in $(\mathcal{O}_F/\mathfrak{Q})^\times/\left((\mathcal{O}_F/\mathfrak{Q})^\times\right)^M$. Therefore κ has order t in $(\mathcal{O}_F/\mathfrak{q}\mathcal{O}_F)^\times/\left((\mathcal{O}_F/\mathfrak{q}\mathcal{O}_F)^\times\right)^M$. Now, (2) follows from the fact that $\phi_{\mathfrak{q}}$ is an isomorphism (Proposition 5.5.6). □

6.2 Bounding A^χ

For this section it is essential to recall the definitions of the χ-isotypical component of the p-part of a module given in Section 3.5.

First prove the following lemma of linear representation of finite abelian groups. It follows from the decomposition of the regular representation of Δ.

Lemma 6.2.1. *Let Δ act on $\mathbb{Q}[\Delta]$ via multiplication giving it a structure of $\mathbb{Q}[\Delta]$-module. If χ is an irreducible representation of Δ, then $\mathbb{Q}[\Delta]^\chi$ is a free $\mathbb{Q}_p$-vector space of rank 1.*

Proof. Let $M = \mathbb{Q}[\Delta]$. Then $M^{(p)} = \mathbb{Q}_p[\Delta]$. It is plain to see

$$\mathbb{Q}_p[\Delta] = \bigoplus_\chi V_\chi$$

where for every irrdeucible χ, V_χ is a one dimensional $\mathbb{Q}_p$-vector space generated by

$$v_\chi = \sum_\sigma \chi(\sigma)^{-1}\sigma$$

with the property that $V_\chi = \{m \in \mathbb{Q}_p[\Delta] : \sigma m = \chi(\sigma)m \text{ for all } \sigma \in \Delta\}$. Note that to prove this statement it is essential that $\mathbb{Q}_p$ contains the $(p-1)$th roots of unity, and therefore $\chi(\sigma) \in \mathbb{Q}_p$ for every σ and every χ.

Using Proposition 3.5.5 (2) it is clear that for a given χ

$$\mathbb{Q}[\Delta]^\chi = V_\chi.$$

□

Combining this lemma and the Dirichlet unit theorem we can determine $\left(\mathcal{O}_F^\times/\mu_F\right)^\chi$:

Proposition 6.2.2. *Let χ be a nontrivial character of Δ. Then $\left(\mathcal{O}_F^\times/\mu_F\right)^\chi$ is a free module of rank 1 over $\mathbb{Z}_p$.*

Proof. Enumerate the elements of Δ as $\Delta = \{\sigma_1, \ldots, \sigma_{p-1}\}$.

There exists a unit η such that every element of $\mathcal{O}_F^\times \otimes \mathbb{Q}$ can be written uniquely as

$$\prod_{i=1}^{p-1} (\eta_i^\sigma)^{a_i}$$

where $\sum_{i=1}^{p-1} a_i = 0$. Therefore, we have the following exact sequence:

$$0 \to \mathcal{O}_F^\times \otimes \mathbb{Q} \to \mathbb{Q}[\Delta] \to \mathbb{Q} \to 0.$$

Moreover, since $\mathbb{Z}_p$ is torsion free (hence flat) and the sequence is Δ-equivariant it is easy to check that we obtain the corresponding exact sequence of isotypical χ-components of the p-parts.

Finally, using that χ is nontrivial, $\mathbb{Q}^\chi = 0$ and the result follows from the fact that $\mathbb{Q}[\Delta]^\chi$ is free of rank one over $\mathbb{Q}_p$ as we saw in Lemma 6.2.1. □

From now on, let $\eta(n, \mathfrak{r}) = \eta_n^{(\mathfrak{a})}(\mathfrak{r})$, for every $n \geq 1$ and $\mathfrak{r} \in \mathcal{R}$, be the euler system of elliptic units. Consider also χ a character of an irreducible representation of Δ.

We can now give the bound of A^χ in terms of the elliptic units. In fact, the result will only depend on $\eta(1, \mathcal{O}) \in F$. Since η is a global unit, we can consider $\eta(1, \mathcal{O})^\chi \in \left(\mathcal{O}_F^\times/\mu_F\right)^\chi$, then we claim that $\#A^\chi$ is lower or equal than the index of $\eta(1, \mathcal{O})^\chi$ in $\left(\mathcal{O}_F^\times/\mu_F\right)^\chi$.

We can express this last statement as follows.

Definition 6.2.3. Let $\mathcal{C}$ be the $\mathbb{Z}[\Delta]$-submodule of $\mathcal{O}_F^\times$ generated by μ_F and $\eta(1,\mathcal{O})$.

Theorem 6.2.4. *Let χ be the character of an irreducible representation of Δ with values in $\mathbb{Z}_p$. Then,*

$$\#A^\chi \leq \#\left(\mathcal{O}_F^\times/\mathcal{C}\right)^\chi$$

Proof. If χ is the trivial character, Proposition 3.5.5 (1) shows that $A^\chi = 0$ and the result is clear. We may assume that χ is nontrivial. From the definition of $\mathcal{C}$ we have the following Δ-equivariant exact sequence

$$0 \to \langle \eta(1,\mathcal{O})\rangle / \left(\langle \eta(1,\mathcal{O})\rangle \cap \mu_F\right) \to \mathcal{O}_F^\times/\mu_F \to \mathcal{O}_F^\times/\mathcal{C} \to 0$$

where $\langle \eta(1,\mathcal{O})\rangle$ is the $\mathbb{Z}_p[\Delta]$-module generated by $\eta(1,\mathcal{O})$. We can take the tensor product by $\mathbb{Z}_p$ and restrict to the χ-isotypical components. Using Proposition 6.2.2 we deduce that $\left(\mathcal{O}_F^\times/\mathcal{C}\right)^\chi$ is a quotient of $\mathbb{Z}_p$. Since $\#A^\chi$ is finite, if this quotient has an infinite number of elements we are done, otherwise we may assume that

$$\left(\mathcal{O}_F^\times/\mathcal{C}\right)^\chi \cong \mathbb{Z}_p/m\mathbb{Z}_p$$

with m an integer of the form $m = p^k$ for some $k \geq 0$. Noting that $\#A^\chi$ is a power of p, choose M, a power of p, such that M/m anihilates A^χ.

List the elements of $\mathrm{Hom}(A^\chi, \mathbb{Z}/M\mathbb{Z}) = \{0, \alpha_1, \ldots, \alpha_k\}$. They will also be seen as elements of $\mathrm{Hom}(A, \mathbb{Z}/M\mathbb{Z})$ in the natural way (recall Proposition 3.5.5 (1)). Using Proposition 6.1.5, we proceed to define inductively a set of classes $\mathfrak{c} \in A$ and elements $\kappa \in F^\times/\left(F^\times\right)^M$. To ease notation denote by $\kappa(\mathfrak{r}) = \kappa_{1,M}(\mathfrak{r})$ for $\mathfrak{r} \in \mathcal{R}_{1,M}$, in particular $\kappa(\mathcal{O}) = \eta(1,\mathcal{O})$.

- For α_1 and $\kappa(\mathcal{O})^\chi$ apply Proposition 6.1.5: let $\mathfrak{q}_1$ prime of K below $\mathfrak{Q}_1$ with ideal class $\mathfrak{c}_1$ in A satisfying conditions (1) and (2) of the proposition.
- For the ith step, let $\mathfrak{r}_{i-1} = \prod_{j\leq i-1}\mathfrak{q}_j$. For α_i and $\kappa(\mathfrak{r}_{i-1})^\chi$ apply Proposition 6.1.5 and let $\mathfrak{q}_i$ be a prime of K distinct to all the previous $\mathfrak{q}_j$ and $\mathfrak{Q}_i$ a prime above $\mathfrak{q}_i$ with ideal class $\mathfrak{c}_i$ in A. These primes satisfy:
  i. $\alpha_i(\mathfrak{c}_i) \neq 0$,
  ii. $[\kappa(\mathfrak{r}_{i-1})^\chi]_{\mathfrak{q}_i} = 0$ and $d\phi_{\mathfrak{q}_i}(\kappa(\mathfrak{r}_{i-1})^\chi) = 0$ if and only if $(\kappa(\mathfrak{r}_{i-1})^\chi)^d \in \left(F^\times\right)^M$.

In order to prove the desired inequality we will first relate $\#A^\times$ with $\mathfrak{c}_i^\chi$. Secondly we will relate m with the elements $\kappa(\mathfrak{r}_i)^\chi$. Finally, using the factorizations of the ideals generated by $\kappa(\mathfrak{r}_i)^\times$ found in the previous chapter it will be possible to relate $\mathfrak{c}_i^\chi$ with $\kappa(\mathfrak{r}_i)^\chi$. This will show the inequality $\#A \leq m$.

1. Note that the elements $\{\mathfrak{c}_i^\chi\}$ generate A^χ. Otherwise, we could define a nontrivial $\alpha : A^\chi \to A^\chi/\langle \mathfrak{c}_1^\chi, \ldots, \mathfrak{c}_k^\chi\rangle \to \mathbb{Z}/M\mathbb{Z}$ in $\mathrm{Hom}(A^\chi, \mathbb{Z}/M\mathbb{Z})$. This is a contradiction because $\alpha = \alpha_i$ for some i and then $\alpha(\mathfrak{c}_i^\chi) \neq 0$. Now, let s_i be the order of $\mathfrak{c}_i^\chi$ in $A^\chi/\langle c_1^\chi, \ldots, c_{i-1}^\chi\rangle$. Using the first theorem of isomorphism and induction it is plain to prove that

$$\#A^\chi = \prod_{i=1}^{k} s_i.$$

2. Let t_i be the order of $\kappa(\mathfrak{r}_i)^\chi$ in $F^\times/\left(F^\times\right)^M$, in particular, $t_i[\kappa(\mathfrak{r}_i)]_{\mathfrak{q}_i} = 0$. Now, Theorem 5.5.9 (2) shows that $[\kappa(\mathfrak{r}_i)^\chi]_{\mathfrak{q}_i} = \phi_{\mathfrak{q}_i}(\kappa(\mathfrak{r}_{i-1})^\chi)$ (here we are also using that $\phi_{\mathfrak{q}}$ is Galois equivariant in order to deal with the χ-components). From here, using ii., we obtain that $t_{i-1} \mid t_i$.

   The relation between the t_i and M is that M/m divides t_0, and hence it divides all the t_i. To prove this choose u^χ a $\mathbb{Z}_p$-generator of $\left(\mathcal{O}_F^\times/\mu_F\right)^\chi$ such that

$$\kappa(\mathcal{O})^\chi = (u^\chi)^m$$

   (this and the following equalities are in $\left(\mathcal{O}_F^\times/\mu_F\right)$).

   Since $(\kappa(\mathcal{O})^\chi)^{t_0}$ is an Mth power, passing to the quotient $\left(\mathcal{O}_F^\times/\mu_F\right)$ there exists $a \in \left(\mathcal{O}_F^\times/\mu_F\right)$ such that

$$(\kappa(\mathcal{O})^\chi)^{t_0} = (u^\chi)^{mt_0} = a^M \tag{6.3}$$

   if we could prove that $a = (u^\chi)^l$ for some l (i.e. $a \in \left(\mathcal{O}_F^\times/\mu_F\right)^\chi$) then $mt_0 = Ml$ and the result would follow. Note that (6.3) implies that $a^M \in (\mathcal{O}_F/\mu_F)^\chi$, hence, for every $\sigma \in \Delta$

$$\sigma a^M = \chi(\sigma) a^M.$$

   Using that $\#\Delta = p-1$ we see that $\chi(\sigma)^M = \chi(\sigma)$, substituting this in the previous equation and taking Mth roots

$$\sigma a = \zeta\chi(\sigma) a.$$

   for some root of unity $\zeta \in \mu_F$. But all these equalities are in $\left(\mathcal{O}_F^\times/\mu_F\right)$ so in fact $\sigma a = \chi(\sigma) a$.

3. Since t_i is the order of $\kappa(\mathfrak{r}_i)^\chi$ there exists $\nu_i \in F^\times/\left(F^\times\right)^M$ such that $\nu_i^{M/t_i} = \kappa(\mathfrak{r}_i)^\chi\zeta$ for some $\zeta \in \mu_F$. Now we will relate the factorization of the principal ideal (ν_i) and the ideal classes $\mathfrak{c}_i^\chi$. First note that

$$\frac{M}{t_i}[\nu_i] = [\kappa(\mathfrak{r}_i)^\chi] \tag{6.4}$$

(recall that [ ] stands for the factorization of ideals modulo M, to review the complete notation see Definition 5.5.1). Note that for every $\mathfrak{q}$ distinct from $\mathfrak{q}_1, \ldots, \mathfrak{q}_i$, Theorem 5.5.9 (1) says that $[\kappa(\mathfrak{r}_i)^\chi]_\mathfrak{q} = 0$. From here

$$(\nu_i) \equiv (\nu_i)_{\mathfrak{q}_1} + \cdots + (\nu_i)_{\mathfrak{q}_i} \mod t_i\mathcal{I} \tag{6.5}$$

On the other hand, as we already said, $[\kappa(\mathfrak{r}_i)^\chi]_{\mathfrak{q}_i}$ has order t_{i-1} therefore $[\nu_i]_{\mathfrak{q}_i}$ has order t_i/t_{i-1}. But (6.4) implies that $[\nu]_{\mathfrak{q}_i} \in (\mathcal{I}_{\mathfrak{q}_i}/M\mathcal{I}_{\mathfrak{q}_i})^\chi$. The structure of $(\mathcal{I}_{\mathfrak{q}_i}/M\mathcal{I}_{\mathfrak{q}_i})^\chi$ is easy to determine: is a cyclic module of order M generated by $\mathfrak{Q}_i^\chi$ (this case is analogous to Example 6.2.1 and it follows from the fact that Δ acts transitively on the prime ideals above $\mathfrak{q}_i$). Hence

$$[\nu_i]_{\mathfrak{q}_i} = u\frac{t_i}{t_{i-1}}\mathfrak{Q}_i^\chi \tag{6.6}$$

for some unit u in $\mathbb{Z}/MZ$.

Combining (6.5) and (6.6)

$$(\nu_i) \equiv u\frac{t_i}{t_{i-1}}\mathfrak{Q}_i^\chi \mod \mathcal{I}_{\mathfrak{q}_1}, \ldots, \mathcal{I}_{\mathfrak{q}_{i-1}}, t_i\mathcal{I}.$$

Reducing this to A^χ, and noting that t_i kills A^χ (because (M/m) divides t_i)

$$0 = \frac{t_i}{t_{i-1}}\mathfrak{c}_i^\chi, \quad \text{in } A^\chi/\langle \mathfrak{c}_1^\chi, \ldots, \mathfrak{c}_{i-1}^\chi\rangle.$$

Therefore, $s_i \mid (t_i/t_{i-1})$ for all $0 < i \leq k$. Taking the product for all i in this range and using that $t_k \mid M$, and $M \mid mt_0$

$$\#A^\chi \mid m.$$

□

Corollary 6.2.5. *With the notation as above, suppose that* $\eta(1,\mathcal{O})^\chi \notin \mu_F^\chi \left((\mathcal{O}_F^\times)^\chi\right)^p$. *Then,* $A^\chi = 0$.

Remark 6.2.6. In the last proof we saw $\eta(1,\mathcal{O})^\chi$ as an element of $\left(\mathcal{O}_F^\times/\mu_F\right)^\chi$. In this case we are considering $\eta(1,\mathcal{O})^\chi \in \left(\mathcal{O}_F^\times\right)^\chi$.

Proof. Since $\eta(1,\mathcal{O})^\chi \notin \mu_F^\chi$ we have

$$\left(\mathcal{O}_F^\times/\mathcal{C}\right)^\chi \cong \mathbb{Z}_p/m\mathbb{Z}_p$$

where m a power of p. If $m > 1$, the class of $\eta(1,\mathcal{O})^\chi$ in $\left(\mathcal{O}_F^\times/\mu_F\right)^\chi \cong \mathbb{Z}_p$ is a multiple of m, in particular a multiple of p. This is precisely $\eta(1,\mathcal{O})^\chi \in \mu_F^\chi \left((\mathcal{O}_F^\times)^\chi\right)^p$which is not possible. Hence $m = 1$ and we are done. □

Chapter 7

Elliptic units and the L-series of the curve

This chapter has an analytic flavor. First of all we define the L-series of an elliptic curve and give an expression for it in terms of Hecke series for the case of an elliptic curve with complex multiplication. Then we use this expression to relate the elliptic units with special values of the L-series. The key result of this part is the $\mathfrak{p}$-adic expansion of the elliptic units obtained in the last section, whose coefficients depend on special values of the L-series. This expression will allow us to relate the algebraic properties of the elliptic units with the value of the L-series at 1.

In the first part we follow [Sil94] Chapter II Section 10. For the second one we follow [Rub99] Chapter 7. There, Eisenstein series are used to connect elliptic units with the L-function. This was already explained in [CW77]. We use this last reference for some proofs that are omitted in Rubin's work.

Fix K an imaginary quadratic field of class number 1. Let $\mathcal{O}$ be its ring of integers.

7.1 The L-series attached to an elliptic curve

Let F be a number field with ring of integers $\mathcal{O}_F$. Let E be an elliptic curve defined over F. We start defining the following quantities that we will need in order to introduce the L-series.

Definition 7.1.1. Let $\mathfrak{P}$ be a prime of F. Define:

1. $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}/\mathfrak{P}$,
2. $q_{\mathfrak{P}} = \#F_{\mathfrak{P}}$,
3. If E has good reduction at $\mathfrak{P}$, $a_{\mathfrak{P}} = q_{\mathfrak{P}} + 1 - \left(\#\tilde{E}(\mathbb{F}_{\mathfrak{P}})\right)$.

We can introduce the so called local L-series.

Definition 7.1.2. Let $\mathfrak{P}$ be a prime of F. Define

$$L_{\mathfrak{P}}(E_{/F}, T) = \begin{cases} 1 - a_{\mathfrak{P}}T + q_{\mathfrak{P}}T^2 & \text{if } E \text{ has good reduction at } \mathfrak{P}, \\ 1 - T & \text{if } E \text{ has split multiplicative reduction at } \mathfrak{P}, \\ 1 + T & \text{if } E \text{ has non-split multiplicative reduction at } \mathfrak{P}, \\ 1 & \text{if } E \text{ has additive reduction at } \mathfrak{P}. \end{cases}$$

And from this define the global L-series.

Definition 7.1.3. The L-series attached to E is defined via the Euler product

$$L(E_{/F}, s) = \prod_{\mathfrak{P}} L_{\mathfrak{P}}(E_{/F}, q_{\mathfrak{P}}^{-s})^{-1}.$$

It is a conjecture that this series has an analytic continuation at the complex plane $\mathbb{C}$. However, for the case that E has complex multiplication this has been proven.

Suppose that E is an elliptic curve defined over K with complex multiplication by $\mathcal{O}$. Let ψ be its Hecke character with conductor $\mathfrak{f}$. We will be able to write the L-series $L(E_{/K}, s)$ in terms of Hecke series that depend on E.

Definition 7.1.4. Let $\chi : \mathbb{A}_K^\times \to \mathbb{C}^\times$ be a Hecke character of conductor $\mathfrak{s}$. Define the Hecke L-series attached to χ as

$$L(\chi, s) = \prod_{\mathfrak{p}} \left(1 - \chi(\mathfrak{p}) q_{\mathfrak{p}}^{-s}\right)^{-1},$$

where the product is over the prime ideals of K. Expanding the Euler product it can be written as

$$L(\chi, s) = \sum_{\mathfrak{b}} \frac{\chi(\mathfrak{b})}{(\mathrm{N}\mathfrak{b})^s},$$

where the sum is over the ideals of $\mathcal{O}$.

Remark 7.1.5. We are using the natural definition for $\chi(\mathfrak{p})$. If χ is unramified at $\mathfrak{p}$, i.e. $\chi(\mathcal{O}_{\mathfrak{p}}^\times) = 1$ we define $\chi(\mathfrak{p}) = \chi(x)$ for $x = (1, \dots, 1, \pi, 1, \dots) \in \mathbb{A}_K^\times$ such that $\mathfrak{p} = (x)$. Otherwise we define $\chi(\mathfrak{p}) = 0$. We extend this definition to all ideals multiplicatively.

In fact, we will also have to work with partial Hecke L-series.

Definition 7.1.6. Let $\chi : \mathbb{A}_K^\times \to \mathbb{C}^\times$ be a Hecke character of conductor $\mathfrak{s}$. Let $\mathfrak{m}$ be an ideal of $\mathcal{O}$ such that $\mathfrak{s} \mid \mathfrak{m}$.

1. Define
$$L_{\mathfrak{m}}(\chi, s) = \sum \frac{\chi(\mathfrak{b})}{(\mathrm{N}\mathfrak{b})^s}$$
where the sum is restricted to $\mathfrak{b}$ coprime to $\mathfrak{m}$. In particular $L_{\mathfrak{s}}(\chi, s) = L(\chi, s)$.

2. If $\mathfrak{c}$ is an ideal of $\mathcal{O}$ coprime to $\mathfrak{m}$, define $L_{\mathfrak{m}}(s, \chi, \mathfrak{c})$ with the same formula as before but the sum restricted to ideals $\mathfrak{b}$ coprime to $\mathfrak{m}$ such that $[\mathfrak{b}, K(\mathfrak{m})/K] = [\mathfrak{c}, K(\mathfrak{m})/K]$. Note that $K(\mathfrak{m})$ is the ray class field modulo $\mathfrak{m}$.

Hecke proved the analytic continuation of Hecke L-series.

Theorem 7.1.7 (Hecke)**.** *Let $\chi : \mathbb{A}_K^\times \to \mathbb{C}$ a Hecke character of conductor $\mathfrak{s}$. Then $L(\chi, s)$ has analytic continuation to the entire complex plane $\mathbb{C}$. Moreover, there is a functional equation relating $L(\chi, s) = L(\chi, N - s)$ for some real number N that depends on χ.*

And the following theorem by Deuring gives us the expression for the L-series attached to E and proves the analytic continuation of $L(E_{/K}, s)$.

Theorem 7.1.8 (Deuring)**.** *The L-series attached to E can be written in terms of Hecke L series that depend on the Hecke character attached to E as*
$$L(E_{/K}, s) = L(\psi, s)L(\bar{\psi}, s).$$

Proof. Let $\mathfrak{p}$ be a prime of K. Since both sides of the equality are defined by Euler products we will check that we have equality at the local factors, i.e.
$$L_{\mathfrak{p}}(E_{/K}, T) = (1 - \psi(\mathfrak{p})T)(1 - \bar{\psi}(\mathfrak{p})T).$$
Theorem 2.3.4 shows that E has either additive or good reduction at $\mathfrak{p}$. If E has additive reduction the equality is clear, since by Proposition 2.5.9, $\psi(\mathfrak{p}) = 0$. For the case that E has good reduction we have to prove
$$q_{\mathfrak{p}} = \psi(\mathfrak{p})\bar{\psi}(\mathfrak{p}), \quad \#\tilde{E}(\mathbb{F}_{q_{\mathfrak{p}}}) = q_{\mathfrak{p}} + 1 - \left(\psi(\mathfrak{p}) + \bar{\psi}(\mathfrak{p})\right).$$
The first equality follows from the fact that $\psi(\mathfrak{p})\mathcal{O} = \mathfrak{p}$. For the second one, Proposition 2.5.11 says that $[\psi(\mathfrak{p})]$ reduces to the $q_{\mathfrak{p}}$-Frobenius endomorphism of $\tilde{E}(\mathbb{F}_{q_{\mathfrak{p}}})$. From here it is standard to calculate the number of points defined over the base field by finding the fixed points by the Frobenius endomorphism.
$$\#\tilde{E}(\mathbb{F}_{q_{\mathfrak{p}}}) = \ker\left(1 - \widetilde{[\psi(\mathfrak{p})]}\right) = \deg\left(1 - \widetilde{[\psi(\mathfrak{p})]}\right) = \deg\left(1 - [\psi(\mathfrak{p})]\right)$$

where we used that the reduction map preserves the degree (see Remark 1.3.9). Now we use that $\deg(1-[\psi(\mathfrak{p})]) = \ker(1-[\psi(\mathfrak{p})])$ and the structure of the torsion points of an endomorphism given in Proposition 2.2.7

$$\deg(1-[\psi(\mathfrak{p})]) = \mathrm{N}(1-\psi(\mathfrak{p}))$$

and we are done. □

Suppose now that E is defined over $\mathbb{Q}$ and it has complex multiplication by $\mathcal{O}$. Our goal is to give an overview about why $L(E_{/\mathbb{Q}}, s) \neq 0$ implies $L(E_{/K}, s) \neq 0$. We will give the main ideas of the proof but we will skip some details. For the complete chain of reasoning see [Sil94] problems 2.30, 2.31 and 2.32.

Remark 7.1.9. We can consider that curve E as a curve defined over K and consider its associated Hecke character $\psi_{E/K}$.

Proposition 7.1.10 (Deuring)**.** *We have* $L(E_{/\mathbb{Q}}, s) = L(\psi_{E/K}, s)$.

Proof. Both series are defined by an infinite Euler product, so we are going to relate the local factors.

1. If E does not have good reduction at a rational prime p, from Theorem 2.6.5 it follows that E has bad reduction (since E has potential good reduction). Therefore $L_p(E_{/\mathbb{Q}}, s) = 1$ which agrees with $\psi_{E/K}(\mathfrak{p}) = 0$ for a prime $\mathfrak{p}$ above p.

2. If E has good reduction at the rational prime p, one can see that either p splits or p is inert.

   If p splits let $\mathfrak{p}$ be a prime of K such that $p\mathcal{O} = \mathfrak{p}\bar{\mathfrak{p}}$. Using Proposition 2.5.11 we see that $\psi_{E/K}(\mathfrak{p})$ reduces to the p-Frobenius endomorphism. Then one can compute the trace of the p-Frobenius endomorphism as we did in the previous theorem. From here it follows that

   $$L_p(E_{/\mathbb{Q}}, s) = (1-\psi(\mathfrak{p})p^{-s})(1-\psi(\bar{\mathfrak{p}})p^{-s}).$$

   For the case where p is inert we outline the proof given in [La87] Chapter 10 Section 4 Theorem 10. We know that $\widetilde{\psi_{E/K}(p)}$ reduces to the p^2-Frobenius endomorphism and $\psi_{E/K}(p)\mathcal{O} = p$. Hence $[\widetilde{\psi_{E/K}(p)}]$ corresponds to multiplication-by-p composed with some automorphism of the reduced curve. We can actually see that $\psi_{E/K}(p) = -p$. This follows from the fact that the reduced curve is defined over $\mathbb{F}_p$, and hence we have a p-Frobenius endomorphism. Noting that it has degree p and taking into account some other considerations one can show that the p-Frobenius corresponds

to $\sqrt{-p}$ in the quaternion algebra of endomorphisms. Hence $\psi_{E/K} = (\sqrt{-p})^2 = -p$. From here it is plain to see that the local factors are equal

$$L_p(E_{/\mathbb{Q}}, s) = 1 + p^{1-2s} = (1 - \psi_{E/K}(p)p^{-2s}).$$

If one can show that the reduced curve is supersingular there is an easier argument. We have that the trace of the p-Frobenius endomorphism is 0. Then, we can then apply [Sil09] Section V Theorem 2.3.1 to deduce that the trace of the p^2-Frobenius endomorphism is $-2p$. From here it follows easily that $\psi_{E/K}(p) = -p$.

□

Proposition 7.1.11. *We have* $L(\psi_{E/K}, s) = L(\bar{\psi}_{E/K}, s)$.

Proof. Following what we did in the previous proof we compare the local factors at primes p where E has good reduction.

If p is inert, we saw in the proof of the previous proposition that $\psi(p) = -p$. Hence $\psi(p) = \bar{\psi}(p)$.

If p splits, let $\mathfrak{p}$ be a prime of K such that $p\mathcal{O} = \mathfrak{p}\bar{\mathfrak{p}}$. One can see that $\bar{\psi}_{E/K}(\mathfrak{p}) = \psi_{E/K}(\bar{\mathfrak{p}})$ and therefore

$$(1 - \psi(\mathfrak{p})q_p^{-s})(1 - \psi(\bar{\mathfrak{p}})q_p^{-s}) = (1 - \bar{\psi}(\bar{\mathfrak{p}})q_p^{-s})(1 - \bar{\psi}(\mathfrak{p})q_p^{-s}),$$

where $q_p = p^2$. □

Corollary 7.1.12. *If* $L(E_{/\mathbb{Q}}, 1) \neq 0$ *then* $L(E_{/K}, s) \neq 0$.

Proof. It follows plainly from Theorem 7.1.8, Proposition 7.1.10 and Proposition 7.1.11 that $L(E_{/K}, s) = L(E_{/\mathbb{Q}}, s)^2$. □

7.2 Eisenstein series and $\Theta_{E,\mathfrak{a}}$

From now on suppose E is defined over K and it has complex multiplication by $\mathcal{O}$. Fix a Weierstrass equation for E and a lattice L such that $\xi : \mathbb{C}/L \to E(\mathbb{C})$, $\xi(z) = (\wp(z), \wp'(z)/2)$ is an isomorphism. Let ψ be the Hecke character attached to E with conductor $\mathfrak{f}$. Fix an ideal $\mathfrak{a}$ prime to $6\mathfrak{f}$ and define $\Theta_{E,\mathfrak{a}}$ and $\Lambda_{E,\mathfrak{a}}$. Since K has class number one we may choose $\Omega \in \mathbb{C}$ such that $L = \mathcal{O}\Omega$, $f \in K$ such that $\mathfrak{f} = \mathcal{O}f$ and $\gamma \in K$ such that $\mathfrak{a} = \mathcal{O}\gamma$.

In this section we introduce the Eisenstein series associated to a lattice and explain their connection with $\Theta_{E,\mathfrak{a}}$.

We must introduce the analytic version of $\Theta_{E,\mathfrak{a}}$.

Definition 7.2.1. $\Theta_{L,\mathfrak{a}} = \Theta_{E,\mathfrak{a}} \circ \xi$.

On the other hand we introduce the Eisenstein series.

Definition 7.2.2. Given $k \in \mathbb{Z}$, $k \geq 1$ define the k-Eisenstein series as

$$E_k(z, L) = \lim_{s \to k} \sum_{\omega \in L} \frac{(\bar{z} + \bar{\omega})^k}{|z + \omega|^{2s}},$$

where the limit means evaluation of the analytic continuation at $s = k$. When $k \geq 3$ we have

$$E_k(z, L) = \sum_{\omega \in L} \frac{1}{(z + \omega)^k}.$$

To connect these functions we will use the following auxiliary functions.

Definition 7.2.3. 1. The Weierstrass σ-function is defined by the product

$$\sigma(z, L) = z^2 \prod_{0 \neq \omega \in L} (1 - z/\omega)\, e^{(z/\omega) + \frac{1}{2}(z/\omega)^2}.$$

It is a holomorphic function at all $\mathbb{C}$ which has simple zeors at $z \in L$. Moreover, those are the only zeros of $\sigma(z, L)$.

2. Define $\zeta(z, L) = \left(\frac{d}{dz}\sigma(z, L)\right)/\sigma(z, L)$. Note that $\wp(z, L) = -\frac{d}{dz}\zeta(z, L)$.

Definition 7.2.4. For the lattice $L \subset \mathbb{C}$ define:

1. $A(L) = \pi^{-1}\text{Area}(\mathbb{C}/L)$,
2. $s_2(L) = \lim_{s \to 0^+} \sum_{0 \neq \omega \in L} \omega^{-2} |\omega|^{-2s}$.
3. $\eta(z, L) = A(L)^{-1}\bar{z} + s_2(L)z$,
4. $\theta(z, L) = \Delta(L) e^{-6\eta(z,L)z} \sigma(z, L)^{12}$.

They allow us to write.

Lemma 7.2.5. *We have* $\Theta_{L,\mathfrak{a}}(z) = \theta(z, L)^{\mathrm{N}\mathfrak{a}}/\theta(z, \mathfrak{a}^{-1}L)$.

Proof. Both are elliptic functions defined at $\mathbb{C}/L$. By Lemma 4.2.1 we have

$$\text{div}\Theta_{L,\mathfrak{a}} = 12\mathrm{N}\mathfrak{a}(O) - 12 \sum_{P \in \mathfrak{a}^{-1}L/L} (P).$$

On the other hand, using the definition of $\theta(z, L)$

$$f = \frac{\theta(z, L)^{\mathrm{N}\mathfrak{a}}}{\theta(z, \mathfrak{a}^{-1}L)} = \frac{\Delta(L)}{\Delta(\mathfrak{a}^{-1}L)} \frac{\sigma(z, L)^{12\mathrm{N}\mathfrak{a}}}{\sigma(z, \mathfrak{a}^{-1}L)^{12}} e^{-6z^2\left(\mathrm{N}\mathfrak{a}s_2(L) - s_2(\mathfrak{a}^{-1}L)\right)}.$$

This allows us to calculate the divisor of f (using the divisor of $\sigma(z, L)$ given in Definition 7.2.3 (1)) and we get that

$$\mathrm{div} f = \mathrm{div}\Theta_{L,\mathfrak{a}}.$$

Therefore, by the theory of elliptic functions $\Theta_{L,\mathfrak{a}} = \lambda f$ for some $\lambda \in \mathbb{C}$. To find λ we can find the first coefficient of the Laurent series of both functions. For $\Theta_{L,\mathfrak{a}}$ it is easy to see that it is $\gamma^{-12}\Delta(L)^{\mathrm{N}\mathfrak{a}-1}$. For f we have to use that the discriminant of a lattice is a modular form of weight 12, therefore $\Delta(\mathfrak{a}^{-1}L) = \gamma^{12}\Delta(L)$. From here it is plain that $\lambda = 1$ and we are done.

□

The Eisenstein series can be expressed in terms of these functions as well.

Lemma 7.2.6. *1.* $E_1(z, L) = \zeta(z, L) - s_2(L)z - A(L)\bar{z}$.

2. $E_2(z, L) = \wp(z, L) + s_2(L)$.

3. For $k \geq 3$

$$E_k(z, L) = \frac{(-1)^{k-1}}{(k-1)!}\frac{d^{k-2}}{dz^{k-2}}\wp(z).$$

Proof. We closely follow [GS].

1. Consider the following function

$$\phi_s(z, L) = \frac{\bar{z}}{|z|^{2s}} + \sum_{0\neq\omega\in L}\left(\frac{\bar{z}+\bar{\omega}}{|z+\omega|^{2s}} - \frac{\bar{\omega}}{|\omega|^{2s}}\left(1 - \frac{sz}{\omega} + \frac{\bar{z}}{\bar{\omega}}(1-s)\right)\right)$$

where the series converges for $\mathrm{Re}(s) > 1/2$. Moreover it is plain to see

$$\lim_{\substack{s\to 1\\ s>1}} \phi_s(z, L) = \zeta(z, L).$$

On the other hand, if $\mathrm{Re}(s) > 3/2$, the series converges absolutely. Rearranging terms we can write

$$\phi_s(z, L) = \sum_{\omega\in L}\frac{\bar{z}+\bar{\omega}}{|z+\omega|^{2s}} + sz\sum_{0\neq\omega\in L}\omega^{-2}|\omega|^{2-2s} + \bar{z}(1-s)\sum_{0\neq\omega\in L}\frac{1}{|\omega|^{2s}} - \sum_{0\neq\omega\in L}\frac{\bar{\omega}}{|\omega|^{2s}}.$$

The last term equals to 0, since the terms corresponding to ω and $-\omega$ cancel. It can be proven that the two first terms have an analytic continuation that is holomorphic at $s = 1$ which correspond, by definition, to $E_1(z, L)$ and $zs_2(L)$. On

the other hand, the analytic continuation of the third term has a simple pole with residue precisely $A(L)^{-1}$.

Therefore, by unicity, the analytic continuation at $s = 1$ of the left hand side has to equal to $\lim_{s\to 1} \phi_s(z, L)$. Therefore

$$\zeta(z, L) = E_1(z, L) + zs_2(L) + A(L)^{-1}\bar{z}.$$

2. The idea of the proof is very similar as in (1). Consider

$$\phi_s(z, L) = z^{-2}|z|^{-2s} + \sum_{0\neq\omega\in L} \left((z-\omega)^{-2}|z-\omega|^{-2s} - (\omega^{-2}|\omega|^{2s})\right).$$

Clearly,

$$\lim_{\substack{s\to 1\\ s>0}} \phi_s(z, L) = \wp(z, L).$$

Moreover, for s large enough we can rearrange the terms and write it as

$$\phi_s(z, L) = \sum_{\omega\in L}(z-\omega)^{-2}|z-\omega|^{-2s} - \sum_{0\neq\omega\in L} \omega^{-2}|\omega|^{-2s}.$$

These terms have analytic continuation. Since the value of the analytic continuation of the left hand side at $s = 1$ has to agree with the limit of $\phi_s(z, L)$ when $s \to 1$

$$\wp(z, L) = E_2(z, L) - s_2(L).$$

3. It is immediate using the expression

$$E_k(z, L) = \sum_{\omega\in L} \frac{1}{(z+\omega)^k}.$$

□

Combining this two lemmas we obtain the desired result.

Proposition 7.2.7. *If $k \geq 1$,*

$$\frac{d^k}{dz^k} \log \Theta_{E,\mathfrak{a}}(z) = 12(-1)^{k-1}(k-1)!(\mathrm{N}\mathfrak{a}E_k(z, L) - E_k(z, \mathfrak{a}^{-1}L)).$$

Proof. Following Lemma 7.2.5 we can write

$$\begin{aligned}\log \Theta_{E,\mathfrak{a}}(z) &= \mathrm{N}\mathfrak{a} \log \theta(z, L) - \log \theta(z, \mathfrak{a}^{-1}L) = \\ &= \mathrm{N}\mathfrak{a}\left(\log \Delta(L) - 6s_2(L)z^2 + 12 \log \sigma(z, L)\right) - \left(\log \Delta(\mathfrak{a}^{-1}L) - 6s_2(\mathfrak{a}^{-1}L)z^2 - 12 \log \sigma(z, \mathfrak{a}^{-1}\right).\end{aligned}$$

where we used that $A(L) = \mathrm{N}\mathfrak{a}A(\mathfrak{a}^{-1}L)$. Now it is easy to calculate the derivative of this function, and using again $A(L) = \mathrm{N}\mathfrak{a}A(\mathfrak{a}^{-1}L)$ and Lemma 7.2.6 (1)

$$\frac{d}{dz}\log\Theta_{E,\mathfrak{a}}(z) = 12\left(\mathrm{N}\mathfrak{a}E_1(z;L) - E_1(z,\mathfrak{a}^{-1}L)\right).$$

The result for every $k > 1$ follows from differentiating in both sides and use Lemma 7.2.6 (2) and (3) to relate the derivatives of the Eisenstein series.

□

7.3 L-series and $\Lambda_{E,\mathfrak{a}}$

Continue with the notation of the previous section.

We start by showing the relation of Eisenstein series with some partial sums of Hecke series. In order to do so we need the following lemma about the Hecke character attached to E.

Lemma 7.3.1. *If $\beta \in \mathcal{O}$ prime to $\mathfrak{f}$, then $\psi(\beta\mathcal{O})/\beta \in \mathcal{O}^\times$. Moreover, if $\alpha \in \mathcal{O}$ such that $\alpha \equiv \beta \mod \mathfrak{f}$. Then*

$$\frac{\psi(\alpha\mathcal{O})}{\alpha} = \frac{\psi(\beta\mathcal{O})}{\beta},$$

Proof. From Proposition 2.5.1 it follows that $\psi(\beta\mathcal{O})\mathcal{O} = (\beta)$. Hence $\psi(\beta\mathcal{O})/\beta \in \mathcal{O}^\times$.

For the second statement let $x = \alpha\beta^{-1}$. We need to see that $\psi(x\mathcal{O}) = x$. Consider the following ideles:

- $x = (x, x, \dots) \in \mathbb{A}_K^\times$,
- $a = (x, 1, 1, \dots) \in \mathbb{A}_K^\times$ where the first component is the infinite component,
- $b = (b_\mathfrak{q}) \in \mathbb{A}_K^\times$ defined as $b_\mathfrak{q} = x$ if $\mathrm{ord}_\mathfrak{q}(x) \neq 0$ and $b_\mathfrak{q} = 1$ otherwise,
- $c = xb^{-1}a^{-1}$.

We therefore have the relation

$$1 = \psi(x) = \psi(a)\psi(b)\psi(c).$$

From the definition of ψ, it is plain to see that $\psi(a) = x^{-1}$, $\psi(b) = \psi(x\mathcal{O})$. Moreover, since $\alpha \equiv \beta \mod \mathfrak{f}$ we get $\psi(c) = 1$. The result follows. □

Proposition 7.3.2. *Let $\mathfrak{m}$ be an ideal of $\mathcal{O}$ divisible by $\mathfrak{f}$ and let $v \in KL/L$ of order exactly $\mathfrak{m}$. Then, for $k \geq 1$*

$$E_k(v, L) = v^{-k}\psi(\mathfrak{c})^k L_\mathfrak{m}(\bar{\psi}^k, k, \mathfrak{c}),$$

where $\mathfrak{c} = \Omega^{-1}v\mathfrak{m}$.

Remark 7.3.3. It is clear that $\bar{\psi}$ has conductor $\mathfrak{f}$. Therefore, $\bar{\psi}^k$ is a Hecke whose conductor is a divisor of $\mathfrak{f}$. For this reason the expression $L_{\mathfrak{m}}(\bar{\psi}, s, \mathfrak{c})$ makes sense according to Definition 7.1.6.

Proof. We can write $v = \alpha\Omega/\mu$ for μ a generator of $\mathfrak{m}$ and $\alpha \in \mathcal{O}$ coprime to $\mathfrak{m}$. Then, for s large enough

$$\sum_{\omega \in L} \frac{(\bar{v} + \bar{\omega})^k}{|v + \omega|^{2s}} = \frac{\mathrm{N}\mu^s}{\bar{\mu}^k} \frac{\bar{\Omega}^k}{|\Omega|^{2s}} \sum_{\omega \in L} \frac{\left(\bar{\alpha} + \bar{\omega}\bar{\mu}/\bar{\Omega}\right)^k}{|\alpha + \omega\mu/\Omega|^{2s}} = \frac{\mathrm{N}\mu^s}{\bar{\mu}^k} \frac{\bar{\Omega}^k}{|\Omega|^{2s}} \sum_{x \in \mathcal{O}} \frac{(\bar{\alpha} + \bar{\mu}\bar{x})^k}{|\alpha + \mu x|^{2s}}$$

where we used that $L = \Omega\mathcal{O}$ for the last equality. This last sum can be rewritten as

$$\sum_{x \in \mathcal{O}} \frac{(\bar{\alpha} + \bar{\mu}\bar{x})^k}{|\alpha + \mu x|^{2s}} = \sum_{\substack{\beta \in \mathcal{O} \\ \beta \equiv \alpha \mod \mathfrak{m}}} \frac{\bar{\beta}^k}{\mathrm{N}\beta^s}.$$

By Lemma 7.3.1, since $\alpha \equiv \beta \mod \mathfrak{m}$ we have

$$\frac{\psi(\alpha\mathcal{O})}{\alpha} = \frac{\psi(\beta\mathcal{O})}{\beta},$$

and $\psi(\beta\mathcal{O})/\beta \in \mathcal{O}^\times$. Thus

$$\bar{\beta} = \frac{\psi(\alpha\mathcal{O})}{\alpha} \bar{\psi}(\beta\mathcal{O}).$$

So we can write

$$\sum_{\substack{\beta \in \mathcal{O} \\ \beta \equiv \alpha \mod \mathfrak{m}}} \frac{\bar{\beta}^k}{\mathrm{N}\beta^s} = \frac{\psi^k(\alpha\mathcal{O})}{\alpha^k} \sum_{\substack{\beta \in \mathcal{O} \\ \beta \equiv \alpha \mod \mathfrak{m}}} \frac{\bar{\psi}(\beta\mathcal{O})^k}{\mathrm{N}(\beta\mathcal{O})^s}.$$

Consider the map

$$\{\beta \in \mathcal{O} \mid \beta \equiv \alpha \mod \mathfrak{m}\} \to \{\mathfrak{b} \subset \mathcal{O} \mid [\mathfrak{b}, K(\mathfrak{m})/K] = [\alpha\mathcal{O}, K(\mathfrak{m})/K]\}, \quad \beta \mapsto \beta\mathcal{O}.$$

Since K has class number one, using the expression for the Artin map of the extension $K(\mathfrak{m})/K$ it is plain to observe that this map is surjective. The map is injective because there are no nontrivial units congruent to 1 modulo $\mathfrak{f}$ (Corollary 2.6.1). Thus

$$\sum_{\substack{\beta \in \mathcal{O} \\ \beta \equiv \alpha \mod \mathfrak{m}}} \frac{\bar{\psi}(\beta\mathcal{O})^k}{\mathrm{N}\beta^s} = \sum_{\substack{\mathfrak{b} \subset \mathcal{O} \\ [\mathfrak{b}, K(\mathfrak{m})/K] = [\alpha\mathcal{O}, K(\mathfrak{m})/K]}} \frac{\bar{\psi}^k(\mathfrak{b})}{\mathrm{N}\mathfrak{b}^s} = L_{\mathfrak{m}}(\bar{\psi}^k, s, \alpha\mathcal{O}).$$

Multiplying all the constants and using that $\mathfrak{c} = \Omega^{-1} v\mathfrak{m} = \Omega^{-1}\alpha\omega\mathfrak{m}/\mu = \alpha\mathcal{O}$ yields

$$\sum_{\omega\in L} \frac{(\bar{v}+\bar{\omega})^k}{|v+\omega|^{2s}} = v^{-k}\psi(\mathfrak{c})^k L_{\mathfrak{m}}(\bar{\psi}^k, s, \mathfrak{c}).$$

Both sides have analytic continuation. Evaluation at $s = k$ gives the desired result. □

At this point we see that the derivative of $\log\Theta_{L,\mathfrak{a}}(z)$ evaluated at points $v \in KL/L$ of order $\mathfrak{f}$ can be written in terms of partial sums of Hecke L-series evaluated at integer points. In order to obtain the complete Hecke L-series we must work with $\Lambda_{E,\mathfrak{a}}$. This observation should motivate the definition of $\Lambda_{E,\mathfrak{a}}$ as a product of transaltes of $\Theta_{E,\mathfrak{a}}$. We now introduce the analytic version of this definition.

Definition 7.3.4. $\Lambda_{L,\mathfrak{a}} = \Lambda_{E,\mathfrak{a}} \circ \xi$.

Lemma 7.3.5. *Let B be a set of ideals prime to $\mathfrak{f}$ such that the Artin map $\mathfrak{b} \mapsto [\mathfrak{b}, K(\mathfrak{f})/K]$ is a bijection from $B \to \mathrm{Gal}(K(\mathfrak{f})/K)$, then*

$$\Lambda_{L,\mathfrak{a}}(z) = \prod_{\mathfrak{b}\in B} \Theta_{L,\mathfrak{a}}(\psi(\mathfrak{b})u + z)$$

where $u = \Omega/f$ is an $\mathcal{O}$-generator of the $\mathfrak{f}$ torsion on K/L.

Proof. Recall the definition of $\Lambda_{E,\mathfrak{a}}$ of Definition 4.1.7. Now we just have to translate the action of $[\mathfrak{b}, K(\mathfrak{f})/K]$ on $E[\mathfrak{f}]$ to multiplication by $\psi(\mathfrak{b})x^{-1}$, where x^{-1} is a finite idele such that $(x) = \mathfrak{b}$ and for every $\mathfrak{p}$ dividing $\mathfrak{f}$ it has $x_{\mathfrak{p}} = 1$. Therefore multiplication by x^{-1} on $E[\mathfrak{f}]$ is trivial and we are done. □

We finally relate the L-series of E with the function that generates elliptic units.

Theorem 7.3.6. *For every $k \geq 1$,*

$$\frac{d^k}{dz^k}\log\Lambda_{E,\mathfrak{a}}(z)|_{z=0} = 12(-1)^k(k-1)!f^k(\mathrm{N}\mathfrak{a} - \psi(\mathfrak{a})^k)\Omega^{-k}L_{\mathfrak{f}}(\bar{\psi}^k, k).$$

Proof. Recall the expresssion of $\Lambda_{E,\mathfrak{a}}(z)$ of Lemma 7.3.5

$$\Lambda_{E,\mathfrak{a}}(z) = \prod_{\mathfrak{b}\in B} \Theta_{E,\mathfrak{a}}(\psi(\mathfrak{b})u + z).$$

Using the formula for the derivatives of the logarithm of $\Theta_{E,\mathfrak{a}}$ of Proposition 7.2.7

$$\frac{d^k}{dz^k}\log\Lambda_{E,\mathfrak{a}}(z)|_{z=0} = \sum_{\mathfrak{b}\in B}\frac{d^k}{dz^k}\log\Theta_{E,\mathfrak{a}}(z)|_{z=\psi(\mathfrak{b})u} =$$

$$= 12(-1)^k(k-1)!\sum_{\mathfrak{b}\in B}\left(\mathrm{N}\mathfrak{a}E_k(\psi(\mathfrak{b})u; L) - E_k(\psi(\mathfrak{b})u; \mathfrak{a}^{-1}L)\right). \quad (7.1)$$

Now we can apply Proposition 7.3.2 with $v = \psi(\mathfrak{b})u$ and the ideal $\mathfrak{m} = \mathfrak{f}$

$$E_k(\psi(\mathfrak{b})u; L) = u^{-k} L_{\mathfrak{f}}(\bar{\psi}^k, 1, \mathfrak{b}).$$

Hence

$$\sum_{\mathfrak{b}\in B} E_k(\psi(\mathfrak{b})u; L) = u^{-k} \sum_{\mathfrak{b}\in B} L_{\mathfrak{f}}(\bar{\psi}^k, 1, \mathfrak{b}) = u^{-k} L_{\mathfrak{f}}(\bar{\psi}^k, 1). \tag{7.2}$$

To compute $E_K(\psi(\mathfrak{b})u; \mathfrak{a}^{-1}L)$ we first note that since $\psi(\mathfrak{a})\mathcal{O} = \mathfrak{a}$ it is easy to see that

$$E_k(z, \mathfrak{a}^{-1}L) = \psi(\mathfrak{a})^k E_k(\psi(\mathfrak{a})z, L)$$

Therefore we can follow the procedure we just did to get

$$E_k(\psi(\mathfrak{a})\psi(\mathfrak{b})u; L) = u^{-k} L_{\mathfrak{f}}(\bar{\psi}^k, 1, \mathfrak{a}\mathfrak{b})$$

and

$$\sum_{\mathfrak{b}\in B} E_k(\psi(\mathfrak{b})u; \mathfrak{a}^{-1}L) = u^{-k}\psi(\mathfrak{a})^k \sum_{\mathfrak{b}\in B} L_{\mathfrak{f}}(\bar{\psi}^k, 1, \mathfrak{a}\mathfrak{b}) = u^{-k}\psi(\mathfrak{a})^k L_{\mathfrak{f}}(\bar{\psi}^k, 1) \tag{7.3}$$

where the last equality holds because the set $\mathfrak{a}B := \{\mathfrak{a}\mathfrak{b}\}_{\mathfrak{b}\in B}$ is also a set of ideals such that the Artin map $B \to \mathrm{Gal}(K(\mathfrak{f})/K)$ is a bijection. Substituting (7.2) and (7.3) into (7.1) yields to the desired result. □

7.4 $\mathfrak{p}$-adic expansion of $\Lambda_{E,\mathfrak{a}}$

Continue with the notation of the previous sections. In addition, choose a prime $\mathfrak{p}$ not dividing $6\mathfrak{a}\mathfrak{f}$, so E has good reduction at $\mathfrak{p}$. In this section we will work with the formal group $\hat{E}$ over the ring $\mathcal{O}_{\mathfrak{p}}$.

As we have discussed, $\Lambda_{E,\mathfrak{a}}$ is a rational function defined over K. Hence, if we choose a minimal Weierstrass model for E with coordinate functions x, y we have $\Lambda_{E,\mathfrak{a}} \in K(x, y)$. We can consider the power series $x(Z) \in Z^{-2}\mathcal{O}_{\mathfrak{p}}[[Z]]$ and $y(Z) \in Z^{-3}\mathcal{O}_{\mathfrak{p}}[[Z]]$ and substitute them on the expression of $\Lambda_{E,\mathfrak{a}}$ obtaining its corresponding power series. We will denote it by $\Lambda_{\mathfrak{p},\mathfrak{a}}(Z) \in K_{\mathfrak{p}}((Z))$ (see the first row of (7.4) below).

The goal of this section is to find the coefficients of $\Lambda_{\mathfrak{p},\mathfrak{a}}(Z)$. We will do so by using the expressions of the derivatives of $\log \Lambda_{E,\mathfrak{a}}(z)$ at $z = 0$ found in the previous section.

Definition 7.4.1. Let $\log_{\hat{E}}(Z) \in Z + Z^2 K_{\mathfrak{p}}[[Z]]$ be the logarithm of $\hat{E}$. Define the operator D acting on $K_{\mathfrak{p}}((Z))$ as

$$D = \frac{1}{\log'_{\hat{E}}(Z)} \frac{d}{dZ}.$$

This operator of the field of power series corresponds with the derivative operator of elliptic functions.

Proposition 7.4.2. *Identify (x, y) with both $(\wp(z), \wp'(z)/2)$ and $(x(Z), y(Z))$. Then the following diagram is commutative*

$$\begin{array}{ccccccc} K(\wp(z),\wp'(z)) & \longleftarrow & K(E) & \longrightarrow & K(x(Z),y(Z)) & \longrightarrow & K_{\mathfrak{p}}((Z)) \\ \downarrow{\scriptstyle \frac{d}{dz}} & & \downarrow & & \downarrow{\scriptstyle D} & & \downarrow{\scriptstyle D} \\ K(\wp(z),\wp'(z)) & \longleftarrow & K(E) & \longrightarrow & K(x(Z),y(Z)) & \longrightarrow & K_{\mathfrak{p}}((Z)). \end{array} \tag{7.4}$$

Proof. Since D and d/dz are derivations we just need to check that the images of $x(Z)$ and $y(Z)$ by D agree with the images of $\wp(z)$ and $\wp'(z)/2$ by $\frac{d}{dz}$. If the curve E has Weierstrass equation

$$y^2 = x^3 + ax + b$$

with $a, b \in K$, the invariant differential $\omega_{\hat{E}}(Z)$ is

$$\omega_{\hat{E}}(Z) = \frac{\frac{d}{dZ}x(Z)}{2y(Z)}.$$

Since $\log_{\hat{E}}(Z) = \int \omega_{\hat{E}}(Z)$

$$Dx(Z) = 2y(Z).$$

Therefore the image of $x(Z)$ by D agrees with the image of $\wp(z)$ by d/dz.

Since both $(x(Z), y(Z))$ and $(\wp(z), \wp'(z)/2)$ satisfy the Weierstrass equation it is plain to deduce that the image of $y(Z)$ by D agrees with the image of $\wp'(z)/2$ by d/dz. □

We can now translate the information about $\Lambda_{L,\mathfrak{a}}(z)$ to $\Lambda_{\mathfrak{p},\mathfrak{a}}(Z)$.

Theorem 7.4.3. *Given $\Lambda_{E,\mathfrak{a}}(z)$ the power series $\Lambda_{\mathfrak{p},\mathfrak{a}}(Z) \in K_{\mathfrak{p}}((Z))$ satisfies:*

1. *It is a unit in the ring $\mathcal{O}[[Z]]$, i.e. $\Lambda_{\mathfrak{p},\mathfrak{a}}(Z) \in \mathcal{O}[[Z]]^\times$,*
2. *for $k \geq 1$*

$$D^k \log \Lambda_{\mathfrak{p},\mathfrak{a}}(Z)|_{Z=0} = 12(-1)^{k-1}(k-1)! f^k \left(\mathrm{N}\mathfrak{a} - \psi(\mathfrak{a})^k\right) \Omega^{-k} L_{\mathfrak{f}}(\bar{\psi}^k, 1).$$

Proof. 1. Up to a nonzero constant, the function $\Lambda_{E,\mathfrak{a}}(P)$ is a product of functions of the form $(x(\psi(\mathfrak{b})S + P) - x(Q))$. Here $S \in E[\mathfrak{f}]$, $\mathfrak{b}$ prime to $\mathfrak{f}$ and $Q \in E[\mathfrak{a}] - O$. Let's first study the power series of these rational functions.

Fix an embedding $\bar{K} \hookrightarrow \bar{K}_{\mathfrak{p}}$ so that we can view $x(R) \in \bar{K}_{\mathfrak{p}}$ for any torsion point R of E. Let $\bar{\mathcal{O}}$ be the ring of integers of $\bar{K}_{\mathfrak{p}}$. Using the expressions of the addition formula

$$x(\psi(\mathfrak{b})S + P) - x(Q) = \frac{(y(P) - y(\psi(\mathfrak{b})S))^2}{(x(P) - x(\psi(\mathfrak{b})S))^2} - x(P) - x(\psi(\mathfrak{b})S) - x(Q).$$

Since $\mathfrak{a}$ is coprime to $\mathfrak{p}$, Lemma 4.1.5 shows that $x(Q) \in \bar{\mathcal{O}}$. Another application of this lemma gives us that $x(\psi(\mathfrak{b})S) \in \bar{\mathcal{O}}$, this is true because $\psi(\mathfrak{b})S$ has order exactly $\mathfrak{f}$ which is coprime to $\mathfrak{p}$. Since $x(\psi(\mathfrak{b})S) \in \bar{\mathcal{O}}$ has positive valuation, by Lemma 1.3.6 we see that $y(\psi(\mathfrak{b})S) \in \bar{\mathcal{O}}$.

In order to compute the power series of $x(\psi(\mathfrak{b})S + P) - x(Q)$ we have to substitue $x(P), y(P)$ by $x(Z), y(Z)$ on the right hand side of this expression. Using the expressions of these two power series and the fact that the valuations of the coordinate functions at Q and $\psi(\mathfrak{b})S$ are positive it is easy to check that

$$\frac{(y(Z) - y(\psi(\mathfrak{b})S))^2}{(x(Z) - x(\psi(\mathfrak{b})S))^2} - x(Z) - x(\psi(\mathfrak{b})S) - x(Q) \in \bar{\mathcal{O}}[[Z]].$$

Moreover, evaluation at $Z = 0$ corresponds to evaluate the original rational function at $P = O$ (since $O \in E_1(K_{\mathfrak{p}})$). Then, Lemma 4.1.5 (3) ensures

$$x(\psi(\mathfrak{b})S) - x(Q) \in \bar{\mathcal{O}}^{\times}.$$

From here we see that all these power series are units, which implies that $\Lambda_{\mathfrak{p},\mathfrak{a}} \in \bar{\mathcal{O}}[[Z]]^{\times}$. We already knew that $\Lambda_{E,\mathfrak{a}}$ is defined over K by Proposition 4.1.8 so we are done.

2. Consequence of Theorem 7.3.6 and Proposition 7.4.2.

□

Chapter 8

The Coates–Wiles Theorem

Recall that K is an imaginary quadratic field with ring of integers $\mathcal{O}$. Let E be an elliptic curve defined over K with complex multiplication by $\mathcal{O}$. Let $\mathfrak{f}$ be the conductor of its associated Hecke character ψ. Suppose that $\mathfrak{p}$ is a prime of K not diving $6\mathfrak{f}$ below the rational prime p. Assume that $p > 7$ and that it splits in K. Denote by $F = K(E[\mathfrak{p}])$, $\mathcal{O}_F$ its ring of integers, $\Delta = \mathrm{Gal}(F/K)$ and A the ideal class group of F. Recall the definition of χ_E of Definition 3.5.1.

In this chapter we use all the previous work to prove the Theorem of Coates and Wiles. As mentioned before, we need to see that for some prime $\mathfrak{p} = \pi\mathcal{O}$, the Selmer group $S_\pi(E_{/K}) = 0$. This prime will be chosen by a Chebotarev argument so that it satisfies the conditions that we state in the first paragraph as well as other restrictions that we will impose in this chapter.

Looking at the conditions derived in the chapter about the Selmer group it is enough to see that (recall Section 3.4 for the definitions of δ_1 and ε):

- $A^{\chi_E} = 0$,
- $\delta_1(\varepsilon) \neq 0$.

The key for seeing this two points is proving that $\eta(1,\mathcal{O})^{\chi_E} \in \left(\mathcal{O}_F^\times\right)^{\chi_E}$ is not a pth power (where $\eta(1,\mathcal{O})$ will be the corresponding elliptic unit for an ideal $\mathfrak{a}$ of $\mathcal{O}$). As we saw in Corollary 6.2.5 this is one of the conditions to prove $A^{\chi_E} = 0$ and with some extra work we will be able to deduce the remaining conditions to complete the proof. Of course, the fact that $\eta(1,\mathcal{O})^{\chi_E} \notin \left(\left(\mathcal{O}_F^\times/\mu_F\right)^{\chi_E}\right)^p$ depends on the value $L(E,1)$, more precisely it will depend on whether $L(\bar{\psi},1)$ is zero or nonzero modulo $\mathfrak{p}$ (recall that p will be chosen by a Chebotarev argument). As explained in the chapter about L-series, we will use the $\mathfrak{p}$-adic expansion of $\Lambda_{\mathfrak{p},\mathfrak{a}}$ to compute $\eta(1,\mathcal{O})$ and see when it is a power of p. Therefore, we will need to work with formal groups in this section.

8.1 Characterization of when $\eta(1,\mathcal{O})^{\chi_E}$ is a pth power

Write $p\mathcal{O} = \mathfrak{p}\bar{\mathfrak{p}}$. Let $\mathfrak{P}$ be the unique prime of F above $\mathfrak{p}$ (see Theorem 2.6.4) and denote by $F_{\mathfrak{P}}$ the the corresponding local field with ring of integers $\mathcal{O}_{F,\mathfrak{P}}$. In order to define the system of elliptic units we also need to fix an ideal $\mathfrak{a}$ coprime to $6\mathfrak{p}\mathfrak{f}$. Now, we will impose an extra condition on $\mathfrak{a}$ (and it will be clear at the end of this section why this condition is important).

Lemma 8.1.1. *There exists a nontrivial ideal $\mathfrak{a}$ prime to $6\mathfrak{p}\mathfrak{f}$ such that $\mathrm{N}\mathfrak{a} \not\equiv \psi(\mathfrak{a}) \mod \mathfrak{p}$.*

Proof. Since $p > 7$, $\#\mathcal{O}^\times < \#(\mathcal{O}/\bar{\mathfrak{p}})^\times$ and hence the reduction map $\mathcal{O}^\times \to (\mathcal{O}/\bar{\mathfrak{p}})^\times$ is not surjective. Therefore, Corollary 2.6.2 ensures that $K(E[\bar{\mathfrak{p}}])/K$ is nontrivial. By class field theory, there exists a prime $\mathfrak{q}$ of K coprime to $6\mathfrak{p}\bar{\mathfrak{p}}\mathfrak{f}$ and an idele $x = (1,\dots,1,\pi',1,\dots) \in \mathbb{A}_K^\times$ with $(x) = \mathfrak{q}$ such that $[x,K]$ is nontrivial on $K(E[\bar{\mathfrak{p}}])$. The action of $[x,K]$ on $E[\bar{\mathfrak{p}}]$ translates to multiplication by $\psi(x)x^{-1}$. Since it is not the identity, we deduce that

$$\psi(\mathfrak{q}) \not\equiv 1 \mod \bar{\mathfrak{p}}$$

where we used that, by definition, $\psi(\mathfrak{q}) = \psi(x)$. This implies

$$\overline{\psi(\mathfrak{q})} \not\equiv 1 \mod \mathfrak{p}.$$

In addition we also have $\psi(\mathfrak{q})\mathcal{O} = \mathfrak{q}$. Therefore, $\psi(\mathfrak{q}) \notin \mathfrak{p}$ so we can multiply by $\psi(\mathfrak{q})$ on both sides to obtain the desired result for $\mathfrak{a} = \mathfrak{q}$. □

Choose $\mathfrak{a}$ satisfying the conditions of Lemma 8.1.1 and consider the system of elliptic units $\eta(n,\mathfrak{r}) = \eta_n^{(\mathfrak{a})}(\mathfrak{r})$, $n \geq 1$ and $\mathfrak{r} \in \mathcal{R}$. In particular recall the definition of $\eta(1,\mathcal{O})$

$$\eta(1,\mathcal{O}) = \Lambda_{E,\mathfrak{a}}(\xi(\psi(\mathfrak{p})^{-1}\Omega)) \in \mathcal{O}_F^\times$$

where $\xi : \mathbb{C}/L \to E(\mathbb{C})$ is an analytic isomorphism and Ω is an $\mathcal{O}$-generator of the lattice L. Therefore we are evaluating $\Lambda_{E,\mathfrak{a}}$ at the torsion point $P = \xi\left(\psi(\mathfrak{p})^{-1}\Omega\right) \in E[\mathfrak{p}]$.

Consider E as a curve defined over $F_{\mathfrak{P}}$.

Lemma 8.1.2. *If $Q = (x,y) \in E[\mathfrak{p}]$ then $Q \in E_1(F_{\mathfrak{P}})$. Moreover, for $Q \neq O$ the valuation of $z = -x/y$ at the prime $\mathfrak{P}$ is 1.*

Proof. Easy consequence of Proposition 4.1.5, that computes the order of the x coordinate of a $\mathfrak{p}$-torsion point, combined with the characterization of $E_1(F_{\mathfrak{P}})$ of Proposition 1.3.6. □

Therefore $P \in E_1(F_\mathfrak{P})$, letting $z = -x/y$ we can compute $\Lambda_{E,\mathfrak{a}}(P)$ using the $\mathfrak{p}$-adic expansion of $\Lambda_{\mathfrak{p},\mathfrak{a}}$ from Theorem 7.4.3.

$$\eta(1, \mathcal{O}) = \Lambda_{\mathfrak{p},\mathfrak{a}}(z) \in \mathcal{O}^\times \subset \mathcal{O}_{F,\mathfrak{P}}^\times.$$

We proceed to construct a morphism $\delta : \mathcal{O}_{F,\mathfrak{P}}^\times \to E[\mathfrak{p}]$ that will allow us to determine when a unit of $\mathcal{O}_{F,\mathfrak{P}}^\times$ is not a pth power.

Definition 8.1.3. Let $\hat{E}[\mathfrak{p}]$ be the image of $E[\mathfrak{p}]$ via the isomorphism

$$E_1(F_\mathfrak{P}) \xrightarrow{\sim} \hat{E}(\mathfrak{P}), \quad (x, y) \mapsto -x/y.$$

of Proposition 1.4.1. This isomorphism restricts to $E[\mathfrak{p}] \xrightarrow{\sim} \hat{E}[\mathfrak{p}]$.

Proposition 8.1.4. *There is a Δ-equivariant isomorphism given by*

$$E[\mathfrak{p}] \xrightarrow{\sim} \hat{E}[\mathfrak{p}] \xrightarrow{1+\cdot} (1 + \mathfrak{P}\mathcal{O}_{F,\mathfrak{P}}) \,/\, \left(1 + \mathfrak{P}^2\mathcal{O}_{F,\mathfrak{P}}\right).$$

Proof. Both the first map, $(x, y) \mapsto (-x/y)$, and the second one are Δ-equivariant.

The injectivity follows from Lemma 8.1.2, since it shows that every nontrivial $Q \in E[\mathfrak{p}]$ is sent to $1 + z$ with $v_\mathfrak{P}(z) = 1$. Finally, the map is a bijection because both sets have the same number of elements: $\mathrm{N}\mathfrak{p} = \mathrm{N}\mathfrak{P}$ (F/K is totally ramified at $\mathfrak{p}$). □

Definition 8.1.5. Define a Δ-equivariant morphism δ as

$$\delta : \mathcal{O}_{F,\mathfrak{P}}^\times \twoheadrightarrow (1 + \mathfrak{P}\mathcal{O}_{F,\mathfrak{P}}) \,/\, \left(1 + \mathfrak{P}^2\mathcal{O}_{F,\mathfrak{P}}\right) \to E[\mathfrak{p}]$$

where the second map is the map of Proposition 8.1.4.

Remark 8.1.6. If $u \in \mathcal{O}_{F,\mathfrak{P}}^\times$ is a pth power, i.e. $u = a^p$ for some $a \in \mathcal{O}_{F,\mathfrak{P}}^\times$

$$\delta(u) = \delta(a^p) = p\delta(a) = 0.$$

Proposition 8.1.7. *$L(E, 1)/\Omega$ is integral at $\mathfrak{p}$. Moreover, $\delta(\eta(1, \mathcal{O})) = 0$ if and only if $L(\bar{\psi}, 1)/\Omega \equiv 0 \mod \mathfrak{p}$.*

Proof. Let $P = \xi(\psi(\mathfrak{p})^{-1}\Omega) = (x, y)$ and $z = -x/y$. Theorem 7.4.3 allows to write $\eta(1, \mathcal{O}) = \Lambda_{\mathfrak{p},\mathfrak{a}}(z)$ for a power series $\Lambda_{\mathfrak{p},\mathfrak{a}}(Z) \in \mathcal{O}_\mathfrak{p}[[Z]]^\times$. The first terms are

$$\Lambda_{\mathfrak{p},\mathfrak{a}}(z) = \Lambda_{\mathfrak{p},\mathfrak{a}}(0) + \Lambda_{\mathfrak{a},\mathfrak{a}}(0)12f(\mathrm{N}\mathfrak{a} - \psi(\mathfrak{a}))\frac{L(\bar{\psi}, 1)}{\Omega}z + O(z^2). \tag{8.1}$$

Since $\Lambda_{\mathfrak{p},\mathfrak{a}}(Z) \in \mathcal{O}_\mathfrak{p}[[Z]]^\times$ we have that $\Lambda_{\mathfrak{p},\mathfrak{a}}(0) \in \mathcal{O}_\mathfrak{p}^\times$. Therefore, using Lemma 8.1.1, $\Lambda_{\mathfrak{p},\mathfrak{a}}(0)12f(\mathrm{N}\mathfrak{a} - \psi(\mathfrak{a}) \in \mathcal{O}_\mathfrak{p}^\times$ which shows that $L(\bar{\psi}, 1)/\Omega$ is integral at $\mathfrak{p}$.

To prove the second part of the statement we need to compute the projection of $\Lambda_{\mathfrak{p},\mathfrak{a}}(z)$ in $(1+\mathfrak{P}\mathcal{O}_{F,\mathfrak{P}})/(1+\mathfrak{P}^2\mathcal{O}_{F,\mathfrak{P}})$. Since $\mathrm{ord}_{\mathfrak{P}}(z)=1$, (8.1) reduces to

$$\eta(1,\mathcal{O}) \equiv \Lambda_{\mathfrak{p},\mathfrak{a}}(0)\left(1+12f(\mathrm{N}\mathfrak{a}-\psi(\mathfrak{a}))\frac{L(\bar{\psi},1)}{\Omega}z\right) \mod \mathfrak{P}^2.$$

Using again that $\Lambda_{\mathfrak{p},\mathfrak{a}}(0)\in\mathcal{O}_{\mathfrak{p}}^{\times}$, expand it as

$$\Lambda_{\mathfrak{p},\mathfrak{a}}(0) = a_0 + a_1\pi + a_2\pi^2 + \cdots$$

for some uniformizer π at the prime $\mathfrak{p}$. But $F_{\mathfrak{P}}/K_{\mathfrak{p}}$ is totally ramified of degree $\mathrm{N}\mathfrak{p}-1$, so $v_{\mathfrak{P}}(\pi)=\mathrm{N}\mathfrak{p}-1>2$. Therefore, $\delta(\Lambda_{\mathfrak{p},\mathfrak{a}}(0))=0$. Hence

$$\mathcal{O}_{F,\mathfrak{P}}^{\times} \to (1+\mathfrak{P}\mathcal{O}_{F,\mathfrak{P}})\,/\left(1+\mathfrak{P}^2\mathcal{O}_{F,\mathfrak{P}}\right), \quad \eta(1,\mathcal{O}) \mapsto 1+12f(\mathrm{N}\mathfrak{a}-\psi(\mathfrak{a}))\frac{L(\bar{\psi},1)}{\Omega}z$$

and the result follows. □

Corollary 8.1.8. *Following the same notation as above,* $L(\bar{\psi},1)/\Omega \not\equiv 0 \mod \mathfrak{p}$ *implies that* $\eta(1,\mathcal{O})^{\chi_E} \notin \left(\left(\mathcal{O}_F^{\times}\right)^{\chi_E}\right)^p$.

Proof. From the Δ-equivariance of δ and Corollary 3.5.6

$$\delta(\eta(1,\mathcal{O})^{\chi_E}) = \delta(\eta(1,\mathcal{O}))^{\chi_E} = \delta(\eta(1,\mathcal{O})).$$

Proposition 8.1.7 shows that $\delta(\eta(1,\mathcal{O}))\neq 0$ so we just need to follow the reasoning of Remark 8.1.6 to conclude. □

8.2 Proof of the Coates–Wiles Theorem

Theorem 8.2.1. *If* $L(\bar{\psi},1)/\Omega \not\equiv 0 \mod \mathfrak{p}$, *then* $A^{\chi_E}=0$.

Proof. By Corollary 8.1.8 we have that $\eta(1,\mathcal{O})^{\chi_E} \notin \left(\left(\mathcal{O}_F^{\times}\right)^{\chi_E}\right)^p$. If we prove that $\mu_F^{\chi_E}=1$ the result will follow from Corollary 6.2.5.

For the sake of contradiction suppose that $\mu_F^{\chi_E}\neq 1$. Hence, since $\mu_F^{\chi_E}\subset\mu_F^{(p)}$, it contains the pth roots of unity, i.e. $\mu_p\subset\mu_F^{\chi_E}$. Now, recall that the Weil pairing gives a G_K-equivariant isomorphism ([Sil09] Chapter III Proposition 8.3)

$$E[p]\cong \mathrm{Hom}(E[p],\mu_p).$$

Since $E[\mathfrak{p}] = E[\mathfrak{p}]^{\chi_E}$ and $\mu_p=\mu_p^{\chi_E}$, any $\mathbb{F}_p$-linear map from $E[\mathfrak{p}]\to\mu_p$ is Δ-equivariant. Using that $E[p]\cong\mathcal{O}/p\cong\mathcal{O}/\mathfrak{p}\oplus\mathcal{O}/\bar{\mathfrak{p}}\cong E[\mathfrak{p}]\oplus E[\bar{\mathfrak{p}}]$ we can produce a nontrivial element of $\mathrm{Hom}(E[p],\mu_p)^{G_K}$. The Weil pairing implies that $E[p]^{G_K}$ is nontrivial. This is a contradiction because $E[p]=E[\mathfrak{p}]\oplus E[\bar{\mathfrak{p}}]$ and $E[\mathfrak{p}]^{G_K}=E[\bar{\mathfrak{p}}]^{G_K}=O$ since $E[\mathfrak{p}]$ and $E[\bar{\mathfrak{p}}]$ are groups of order p that are not contained in $E(K)$ by Corollary 2.6.2 (note that $p>7$). □

In order to complete the proof of the Coates Wiles–Theorem we need to see that $\delta_1(\varepsilon) \neq 0$. Recall that $\delta_1 : F_{\mathfrak{P}}^{\times} \to E[\mathfrak{p}]$ and we already proved that $\delta_1(\mathcal{O}_{F,\mathfrak{P}}^{\times}) = E[\mathfrak{p}]$ (Proposition 3.4.9).

Proposition 8.2.2. *Suppose that p splits over K and $\mathrm{Tr}_{K/\mathbb{Q}}\psi(\mathfrak{p}) \neq 1$. Then,*

1. *$\mu_p \not\subset F_{\mathfrak{P}}$,*
2. *$\left(\mathcal{O}_{F,\mathfrak{P}}^{\times}\right)^{\chi_E}$ is free of rank one over $\mathbb{Z}_p$.*

Proof. 1. We prove the contrapositive statement. Suppose that $\mu_p \subset F_{\mathfrak{P}}$, since p splits over K, by elementary ramification theory $F_{\mathfrak{P}} = K_{\mathfrak{p}}(\mu_p)$. Class field theory shows that $[p, \mathbb{Q}_p(\mu_p)/\mathbb{Q}_p] = 1$, so using the functoriality of the local Artin map $[p, F_{\mathfrak{P}}/K_{\mathfrak{p}}] = 1$.

Moreover, we have that $[\psi(\mathfrak{p}), F_{\mathfrak{P}}/K_{\mathfrak{p}}] = 1$. Indeed, $\psi(\mathfrak{p}) = \psi(x) = \alpha(x)$ for the finite idele $x = (1, \dots, 1, \pi, \dots) \in \mathbb{A}_K^{\times}$. We have that $[x, K]$ acts on $E[\mathfrak{p}]$ as multiplication by $\alpha(x)x^{-1} \in \mathcal{O}_{\mathfrak{p}}^{\times}$. Similarly, and noting that $\psi(\alpha(x)x^{-1}) = 1$ because E has good reduction at $\mathfrak{p}$ we note that $[\alpha(x)x^{-1}, K]$ acts on $E[\mathfrak{p}]$ as multiplication by $\alpha(x)^{-1}x$. From here, using the relation between the local and global Artin map:

$$[\psi(\mathfrak{p}), F_{\mathfrak{P}}/K_{\mathfrak{p}}] = [\alpha(x), F_{\mathfrak{P}}/K_{\mathfrak{p}}] = [\alpha(x)x^{-1}, F_{\mathfrak{P}}/K_{\mathfrak{p}}][x, F_{\mathfrak{P}}/K_{\mathfrak{p}}] = 1.$$

Therefore, $[p/\psi(\mathfrak{p}), F_{\mathfrak{P}}/K_{\mathfrak{p}}] = 1$. Since $p/\psi(\mathfrak{p}) \in \mathcal{O}_{F,\mathfrak{P}}^{\times}$ fixes a totally ramified extension of degree $p-1$, by local class field theory

$$p/\psi(\mathfrak{p}) \equiv 1 \mod \mathfrak{p}.$$

From here

$$\mathrm{Tr}_{K/\mathbb{Q}}\psi(\mathfrak{p}) = \psi(\mathfrak{p}) + \overline{\psi(\mathfrak{p})} = \psi(\mathfrak{p}) + p/\psi(\mathfrak{p}) \equiv 1 \mod \mathfrak{p}.$$

Since $|\psi(\mathfrak{p})| = \sqrt{p}$, $|\mathrm{Tr}_{K/\mathbb{Q}}\psi(\mathfrak{p})| < 2\sqrt{p} < p-1$ and hence $\mathrm{Tr}_{K/\mathbb{Q}}\psi(\mathfrak{p}) = 1$.

2. Denote by $U^{(n)}$ the nth higher unit group of $\mathcal{O}_{F,\mathfrak{P}}^{\times}$. Since $\mathcal{O}_{F,\mathfrak{P}}^{\times} \otimes \mathbb{Z}_p \cong U^{(1)} \otimes \mathbb{Z}_p$ it is enough to prove the result for $\left(U^{(1)}\right)^{\chi_E}$.

It is well known that, for n large enough, the logarithm map gives a Δ-equivariant isomorphism $U^{(n)} \cong \mathcal{O}_{F,\mathfrak{P}}$. Taking a $\mathcal{O}_{\mathfrak{p}}$-basis of $\mathcal{O}_{F,\mathfrak{P}}$ one can define a Δ-equivariant isomorphism (normal basis theorem) $\mathcal{O}_{F,\mathfrak{P}} \otimes \mathbb{Q}_p \cong K_{\mathfrak{p}}[\Delta]$. We therefore obtain

$$U^{(n)} \otimes \mathbb{Q}_p \cong K_{\mathfrak{p}}[\Delta]$$

a Δ-equivariant isomorphism. And now, from the exact sequence

$$0 \to U^{(n)} \to U^{(1)} \to U^{(1)}/U^{(n)} \to 0$$

and using that $U^{(1)}/U^{(n)}$ is finite we get a Δ-equivariant isomorphism

$$U^{(1)} \otimes \mathbb{Q}_p \cong U^{(n)} \otimes \mathbb{Q}_p.$$

Combining these observations and taking χ_E-components, $\left(U^{(1)} \otimes \mathbb{Q}_p\right)^{\chi_E} \cong K_{\mathfrak{p}}[\Delta]^{\chi_E}$ which is free of rank 1 over $\mathbb{Q}_p$ (analogous to Lemma 6.2.1). The result follows from (1), where we proved that $U^{(1)}$ contains no elements of p torsion (in fact it is torsion free).

□

Theorem 8.2.3. *Suppose that* $L(\bar{\psi}, 1)/\Omega \not\equiv 0 \mod \mathfrak{p}$ *and that* $\mathrm{Tr}_{K/\mathbb{Q}}\psi(\mathfrak{p}) \neq 1$. *Then the natural morphism between* $\mathbb{Z}_p$*-modules*

$$(\mathcal{O}_F)^{\chi_E} \to \left(\mathcal{O}_{F,\mathfrak{P}}^{\times}\right)^{\chi_E}$$

is an isomorphism.

Proof. The injectivity is clear since we are taking χ_E-components of the inclusion map $\mathcal{O}_F^{\times} \hookrightarrow \mathcal{O}_{F,\mathfrak{P}}^{\times}$.

For the surjectivity, note that Corollary 8.1.8 shows that the image of $\eta(1, \mathcal{O})^{\chi_E}$ is not a pth power. Since $(\mathcal{O}_{F,\mathfrak{P}})^{\chi_E}$ is a free module of rank one over $\mathbb{Z}_p$, $\eta(1, \mathcal{O})^{\chi_E}$ generates this module. □

Theorem 8.2.4. *Suppose that* $L(E_{/K}, 1) \neq 0$. *Then* $E(K)$ *is finite.*

Proof. Theorem 7.1.8 ensures that if $L(E_{/K}, 1) \neq 0$ then $L(\bar{\psi}, 1) \neq 0$. By the Chebotarev Theorem there are infinite primes $\mathfrak{p}$ of K above a rational prime p such that p splits in K and $\mathrm{Tr}_{K/\mathbb{Q}}\psi(\mathfrak{p}) \neq 1$. We can choose one such that:

- $p > 7$,
- $\mathfrak{p}$ coprime to $6\mathfrak{f}$,
- $L(\bar{\psi}, 1)/\Omega$ is a unit at $\mathfrak{p}$.

Therefore we can apply the previous results of this chapter to $\mathfrak{p}$. By Theorem 8.2.1, $A^{\chi_E} = 0$. In addition, Theorem 8.2.3 shows that $\eta(1, \mathcal{O})$ generates $\mathcal{O}_{F,\mathfrak{P}}^{\times}$. Since $\delta_1(\mathcal{O}_{F,\mathfrak{P}}^{\times}) = E[\mathfrak{p}]$, it has to be $\delta_1(\eta(1, \mathcal{O})) \neq 0$. Thus, $\delta_1(\varepsilon) \neq 0$.

The conditions of Corollary 3.4.12 are satisfied so we can affirm $S_\pi(E_{/K}) = 0$, where $\pi \in \mathcal{O}$ such that $\mathfrak{p} = \pi\mathcal{O}$. Therefore $E(K)/\mathfrak{p}E(K) = 0$ so by the Mordell–Weil Theorem $E(K)$ has to be finite (Corollary 3.1.2). □

Corollary 8.2.5. *Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by $\mathcal{O}$. If $L(E_{/\mathbb{Q}}, 1) \neq 0$ then $E(\mathbb{Q})$ is finite.*

Proof. Corollary 7.1.12 shows that $L(E_{/\mathbb{Q}}, 1) \neq 0$ implies that $L(E_{/K}, 1) \neq 0$. By Theorem 8.2.4 we have that $E(K)$ is finite. Since $E(\mathbb{Q}) \subset E(K)$ the result follows. □

References

[AM69] M. Atiyah and I.G. MacDonald. *Introduction to commutative algebra*. Reading, Mass, 1969.

[CS06] John Coates and Ramdorai Sujatha, *Cyclotomic fields and zeta values*. Springer Science & Business Media, 2006.

[CW77] John Coates and Andrew Wiles, On the conjecture of Birch and Swinnerton-Dyer. *Inventiones math.* **39**, 223-251, 1977.

[GS] Catherine Goldstein and Norbert Schappacher, Séries d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe. *J. reine angew. Math* **327** (1981) 184-218.

[La87] Serge Lang, *Elliptic functions*. Springer-Verlag, New York, 1987.

[Mil13] James S. Milne, *Class Field Theory (v4.02)*. Avaliable at `www.jmilne.org/math/`, 2013.

[Neu13] Jurgen Neukirsh, *Algebraic number theory*. Graduate Texts in Mathematics, **332**. Springer Science & Business Media, 2013.

[Poo] Bjorn Poonen, *A brief summary of the main statements of class field theory*. Avaliable online at `http://www-math.mit.edu/ poonen/`.

[Rub00] Karl Rubin *Euler Systems*. Princeton University Press, 2000.

[Rub99] Karl Rubin, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, Arithmetic theory of elliptic curves (Cetraro, 1997), 167–234, Lecture Notes in Math., **1716**, Springer, Berlin, 1999.

[Sam70] Pierre Samuel, *Algebraic Theory of Numbers Translated by Allan J. Silberger*. Corporation 2013.

[Ser13] Jean-Piere Serre, *Local fields*. Graduate Texts in Mathematics, **67**. Springer Science & Business Media, 2013.

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*. Graduate Texts in Mathematics, **106**. Springer Science & Business Media, 2009.

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*. Graduate Texts in Mathematics, **151**. Springer Science & Business Media, 1994.